Global Information Assurance Certification Paper

Web Bugs
Kimberly Craig
October 22, 2000

Web Bugs are tiny one pixel graphic images that are hidden on a website, in E-mail messages, Microsoft Word documents, Excel spreadsheets and Powerpoint documents or any other HTML based word processing application. Web Bugs can also be hidden in newsgroup postings. Web Bugs are used by advertising companies to track and monitor website visitors identifiable by their IP addresses. They can be used in conjunction with "cookies" to profile Internet surfers and their viewing habits. Web Bugs are use by marketing companies in E-mail campaigns. Authors and / or corporations to monitor proprietary documentation can also use web Bugs.

Web Bugs have many uses, both beneficial and malicious, and are potentially harmful to online privacy.

According to Richard M. Smith, an advocate of online privacy, "A Web Bug" is a graphics on a Web page or in an E-mail message that is designed to monitor who is reading the Web page or E-mail message…They are represented as HTML IMG tags." Web Bugs differ from invisible alignment GIFs by the simple fact that a "Web Bug will be typically loaded from a different Web server than the rest of the page…." Web Bugs are the size of a period or dot on a page.

When visiting a Web site that has a hidden Web Bug, information such as the IP address of the computer, the URL of the visited Web site, the time, any corresponding cookie values, and the type of browser and operating system in use is transmitted to the host server. The Web Bug sends a message to the server notifying it of its location and identity. In order to communicate with each other, Web Bugs and cookies have to originate from the same source, i.e., the same advertising agency server. According to Helen Bradley, "Over time, an advertising agency with a significant presence on the Web (a network of client sites) can build up a detailed profile of your browsing habits. The result will be that you are likely to see that the advertising served up on the Web sites you visit is closely aligned to your personal preferences because the advertising agency knows a lot about the sites you visit and what you view based on the information it has stored on you." Most people are aware of cookies and the fact they are being tracked; however, people are not aware of these hidden Web Bugs and have no idea they are still being monitored.

If this much information about Internet users can be collected and stored on a server located on the Internet, the day is not far away when this information can be tied together with a name, address, phone and possibly credit card information. It won't be long until another hacker figures out how to access this valuable information and use it to his advantage. Online privacy and vendor responsibilities are currently hot topics in congressional debates. Privacy advocates are demanding that advertising and marketing companies disclose the fact that this information is being collected and for what purpose,

and more importantly how this information is being safeguarded. Also, surfers should have the right to deny information from being collected. It is in an Internet surfer's best interest to read the privacy policies of the sites visited.

Web Bugs hidden in E-mail and newsgroup postings can indicate who received it, who read it and if the E-mail was forwarded. Marketing companies can send out mass E-mailings and track the interest generated. Richard Smith, in his Web Bug FAQ, states that Web Bugs are used in this way " 1. To measure how many people have viewed the same E-mail message in a marketing campaign. 2. To detect if someone has viewed a …E-mail message or not. People who do not view a message are removed from the list for future E-mailings. 3. To synchronize a Web Browser cookie to a particular E-mail address. This trick allows a Web site to know the identity of people who come to the site at a later date." In order for a Web Bug to work in a newsgroup posting, they have to be accessed by Outlook Express or Netscape Messenger. Richard Smith again states that "a Web Bug can be used to log people who are reading messages in a particular group. Such bugs might be used for example by investigators to track illegal activity…. Web Bugs might also be used to monitor people in extreme political groups."

Word allows the embedding of an image location instead of the actual image as a space-saving technique. Web Bugs embedded in Word documentation do not need the use of stored cookies in order to access a remote server via the Web. The embedded code reaches out to the server to retrieve the graphic image, thus initiating the logging that allows the author to track the IP address and hostname of the person accessing the document, how often it is opened, and if any portion of it is copied into another file. Cutting and pasting will also transfer the bugs. Anyone who opened one of these documents would not know that the Web bug was embedded in the document. According to Mr. Smith, "Web Bugs in Word documents could be used to detect and track leaks of confidential documents from a company, uncover possible copyright infringement of newsletters and reports, monitor press release distribution, and track the quoting of text when it is copied from one Word document to another;" thus allowing the author of a document to bug and monitor his work.

To uncover a Web Bug on a website, wait for the page to load then view the source code. In Netscape click on View, then page source; in Internet Explorer, click on View then Source; search the resulting page for an IMG tag with the attributes WIDTH=1 HEIGHT=1 BORDER=0 and SRC= http://…. This is the embedded code indicative of a Web Bug especially if it includes a source pointer to a server in a different location than where the page source loaded from. The code is similar in E-mail and documents, however, the users IP address will be included as well as the URL to where the hidden Image is actually located.

There are several methods to prevent Web Bugs from transmitting information about a user over the Internet. One source is www.junkbusters.com which provides a free software program the user can install and configure to block unwanted advertising media from accessing their computer. Most ad blocking software will deter cookies.

Another way is to configure the browser to notify the user when a cookie is being placed on the computer, therefore allowing the user to decline or accept the cookie. Or set the browser security at the highest level to not accept cookies at all. However, adblocking software will not detect the presence of Web Bugs, and most users access sites where they need to be identified to the server by some method, so turning off cookies is not the best solution. Installing a personal firewall wall that blocks malicious code from accessing the users computer from the Internet is one of the best options. Zone Labs, Zone Alarm personal firewall notifies users when applications attempt to access the Internet, also allowing the user to decline or accept the connection. Educating users
Of the potential dangers of privacy data violations existing on the Internet is probably the best deterrent. The more aware people are of what transpires behind the scenes, the less likely Online companies will take advantage of them and misuse the information.

Bradley, Helen "Beware Of Web Bugs & Clear GIFs" April 2000•PC Privacy Volume 8, Issue 4
http://www.smartcomputing.com/editorial/article.asp?article=articles/archive/g0804/11g04/11g04.asp&guid=q6ozaqyk(18 Oct. 2000)

Festa, Paul and Barnes, Cecily "Word documents susceptible to "Web Bug" infestation" August 2000 http://news.cnet.com/news/0-1005-200-2652562.html (18 Oct. 2000)

Kelsey, Dick "Some Microsoft Documents May Be Web Bugged" September 2000
http://www.computeruser.com/news/00/09/05/news4.html (18 Oct. 2000)

Olsen, Stefanie. " Nearly undetectable tracking device raises concern" July 2000
http://news.cnet.com/news/0-1007-200-2247960.html (18 Oct. 2000)

Powell Crowe, Elizabeth. "Is Your Browser Being Bugged?" February 2000
http://www.computeruser.com/magazine/national/1804/intb1804.html (18 Oct. 2000)

Smith, Richard. "The Web Bug FAQ." November 1999
http://www.tiac.net/users/smiths/privacy/wbfaq.html (18 Oct. 2000)

Last Updated: October 22nd, 2017

Upcoming Training

SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event