

Google – Friend or Foe?

The growth of Google as the default search engine on the Internet has made Google one of the most amazing success stories of the Internet age.

Many were sceptical of their original share price at launch day, but their continued success at a financial level has silenced many of these.

One of the downsides of the dramatic growth of Google and its massive data centre infrastructure is the amount of data that is available in one location that could assist the malicious user.

The “Googleplex” as the massive number of servers running the Google suite of applications is known is rumoured to consist of more than 500,000 spread in huge data-centres world-wide. Google has maintained a policy from the outset of assembling their own servers and racking systems and as a result they are actually one of the largest server manufacturers in the world today!

Over the last number of years, this vast amount information that has been trawled from web sites around the world and indexed has been mined for the malicious purposes.

Potential hackers have worked out that if you enter certain search words and use Google’s own search language operators you can gather a tremendous amount of information. Depending on how badly the target web site has been designed, information such as passwords, configuration files and databases of information can be available from the search.

One of the issues is that this process can take place without ever accessing the target web site infrastructure. A hacker does not have to access a web service to gather information as a precursor to an attack, thereby reducing the likelihood of being detected by security systems at the target site. The Googleplex also caches this information in its massive data storage facilities and will continue to make that cached information available long after the web site in question has remedied the situation. This may often result in a password that was available via a search no longer being available, the site operator choosing not to change the password as it is no longer searchable but the cache in Google still has it so the risk continues.

This information has become so useful to the hacking community that it is also now a standard component in the Information Gathering phase for most Penetration Tests that have been commissioned by a customer.

Another unfortunate side effect of this incredible cache of information created and managed by Google is the accessibility of Internet connected digital web cameras. Many people have implemented a web-cam to monitor security at a particular location, many crèches have them installed, university students install in their rooms to talk to friends etc across the Internet and so on. Effectively, most of these devices are actually accessed as a web page and are thus cached by Google. There have been many incidents, often viewed as being quite humorous, where people from all around the world have been able to access a web-cam presumed to be used privately between two people! However, there is a very serious and dark side to this

and that is where someone could access the video stream from a web-cam in someone's private office, living room, bed room etc without the owner realising this. This could be a huge invasion of one's privacy. As these cameras are often used for physical security purposes, a criminal could determine when the premises are unattended, figure out the routines of security guards etc and use that information to commit a crime.

As these cameras have become more powerful with greater picture resolution, enhanced night vision with infrared LEDs and the ability to control the Pan, Tilt and Zoom (PTZ), the spectre of privacy invasion and stalking looms larger. The ability to access the PTZ controls of a web cam means that no area within the field of view is safe. These controls are accessible from the web page that displays the image from the camera.

The message from this is that a facility such as Google is an essential part of most people's Internet experience, and overall the Internet has to be seen as a better, more accessible place as a result of Google and other search engines. However, because of the potential for misuse of the massive cache databases people must be vigilant when connecting any device to the Internet. Once a new web service appears on the Internet and is cached by Google, all its accessible information is now searchable by any Internet user. Web sites should be tested to ensure no unnecessary or sensitive information is available on the site for the web search engines to cache.

Rits Group Head Quarters
Information Security Centre
2052 Castle Drive
Citywest Business Campus
Co. Dublin
Ireland

Tel: +353 (0) 1 6420500
Fax: +353 (0) 1 4660468
Email: info@ritsgroup.com
Web: www.ritsgroup.com