techday

Submit your content

From the Magazine

The unwelcome guest in your machine 0

By Contributor, Saturday, 1st August, 2009

Web applications (apps for short): they're such handy little things and there are literally thousands of them out there, just waiting for you to download.

They can range from tools that augment your browser's functions, to media players, text readers, word processors and much more. You can add them to your computer with just a click.

But did you ever stop to wonder just what else you're bringing into your computer with that download? Web applications are a major source of malware – not just written in by dodgy software dealers, but by creating vulnerabilities for hackers to exploit.

These types of security breaches were the focus of a recent presentation at the first OWASP (Open Web Application Security Project) Day, a conference entirely dedicated to Web application security.

Paul Craig, Principal Security Consultant at Security-Assessment.com, asked the question: "Why is the Internet still insecure?".

"I have zero faith personally in the trust of the Internet," he told the conference. "If it was up to me I would rather have my money under my mattress, I wouldn't use online banking and I wouldn't touch anything to do with a computer."

In his research for his presentation, Craig (who calls himself "a devoted hacker") examined vulnerabilities detected by Security-Assessment. com five years ago compared with those detected today.

"The first security policies were actually outlined in the 1980s – they said pretty much what we say now: account and password management are very important, users need to choose secure passwords – they're really the crux of your security. Privilege separation is really good [administrator access], and it's very important to use encryption wherever possible. A shocking thing is that less than 10% of the Web applications we review today actually adhere to these principles."

In recent years Web apps have become the tool of choice for hackers because they weren't regarded as a security risk. Web apps were easy to write, they were being widely offered online, and the writers paid little or no heed to security.

"All of a sudden those Web applications you didn't know anything about are now the number one way you can break into someone's network," says Craig.

Poorly wriiten applications allow a hacker to fiddle remotely with the script of a Web page – a process known as 'injection'. The hacker creates a piece of code which is then injected into the page; thus the page becomes 'infected'. This infection can then be spread to the computer of any Web user who clicks onto that page. They may be redirected to a site of the hacker's choosing, where their computer will then download malware. This could steal confidential information from their computer (including cached passwords or credit card details), or make their computer part of a botnet of compromised machines used to deliver spam and malware.

Around 2004-2005, experts at Security-Assessment.com estimated that 75% of Web apps were vulnerable to injection attacks. Even today, at least one critical vulnerability (where a system has been completely compromised) is being detected every hour.

Web 2.0 applications (interactive, audio and video) are everywhere now. They're increasingly complex and therefore more likely to contain loopholes. In addition, virtually every business has a Web presence now; more and more people are banking and shopping online, and it only takes one lapse to allow cybercriminals to grab account and/or credit details.

Web developers, in Craig's opinion, are failing the consumer. They write an application for a customer, but whether it's secure from intrusions is usually not answered until a vulnerability is detected – generally after a hacker has found and exploited it.

Craig keeps finding broken access controls which can be bypassed, passwords that can be easily guessed; and don't get him started on files ("developers fail pretty much anything to do with files").

So how can ordinary users protect themselves from this type of intrusion? It's difficult, unless you're pretty tech-savvy. NetGuide has often warned about the risks posed by compromised Web pages; it can even happen o sites you trust and visit regularly. Unexpected invitations to click on links are usually a warning sign, and if you run your cursor across a link you should be able to read it and tell whether it's legitimate. An extra-long URL is a good indication that something is wrong, although that's not foolproof.

Always use encryption when carrying out any online financial transaction – the site should do this as a matter of ourse (look for the padlock icon). Also, beforeyou download that handy-looking application, ask yourself whether you really need it.

For the more technically minded, setting up a virtual machine (VM) in your computer is the answer. This creates a second operating system, and it's from there that you browse Web pages and upload any new applications. If something looks wrong, you just delete the VM and your original system is unaffected. For more, see tinyurl.com/m994en and www.vmware.com (Windows 7 Ultimate will have a virtual PC built in).

We're not trying to scare you; we're simply pointing out that there are scary things on the Web, and sometimes the worst threat is the one you invite in yourself.

"The Internet definitely is getting better," says Paul Craig. "It's getting more secure but it's not there yet, because there was still at least one critical finding in every application we reviewed, so I only really need one bug to get in."

Like DISQUS

Add New Comment

Type your comment here.

Post as ...

Showing 0 comments

Sort by Newest first Subscribe by email Subscribe by RSS

Our hottest keywords

iPad	Telecom XT	Apple
Microsoft Office	3G	Adobe
Vodafone	Ingram Micro	Renaissance
Google	Fibre	Cloud

Join the 81,981 people following TechDay

Twitter Facebook LinkedIn RSS Email

Partners

Project Management Software