Yahoo Accounts Hijacked via XSS-Type Attack

Yahoo Accounts Hijacked via XSS-Type Attack

SYDNEY/AUCKLAND – January 31, 2013 – Popular webmail provider Yahoo has been slammed with a new e-mail-based attack that seizes control of victims' accounts. Bitdefender Labs discovered the ongoing campaign today and are once again warning users about the dangers of clicking spammy links.

The account hijacking begins with a spam message with a short link to an apparently harmless session of the reliable news channel MSNBC (hxxp://www.msnbc.msn.com-im9.net[removed]).

A closer look at the real link reveals that the true domain is not part of MSNBC, but a crafty domain composed of subdomains at hxxp://com-im9.net.

The domain was registered in Ukraine on Jan 27 and is hosted in a data center in Nicosia, Cyprus. This page contains a piece of malicious JavaScript, disguised as the popular Lightbox library that will perform the attack in stage 2.

Before we proceed, let's see what cookie theft is all about: security on the web is based on what we call the same-origin policy, a complex mechanism that won't allow Site A to access resources of Site B, such as cookies. Cookies are small snippets of text created when the user logs into a system, and they are used to (among other things) remember that the account holder has already passed the authentication once. Otherwise, the user will have to log in whenever they read another e-mail or when they navigate from one page to another. So, in this context, it is obvious that a piece of code running on Site A can't steal a cookie set by Site B. However, a subdomain of Site B can access the resources of Site B, and this is what the attackers did.

The second stage of the attack is focused on the Yahoo Developers Blog (developers.yahoo.com), which conveniently uses a buggy version of WordPress. More to the point, they exploit the SWF Uploader of the WordPress platform at http://developer.yahoo.com/blogs/ydn/wp-includes/js/swfupload/swfupload.swf. It has a security flaw known as CVE-2012-3414 (by the way, it has been patched since WordPress version 3.3.2).

Since it is located on a sub-domain of the yahoo.com website, all the attackers need to do is trigger the bug and pass a command that steals the cookie, and then send it "home".

At this point, miscreants have full access to the victim's contact list until the current session expires or the user logs out. Crooks will either spam the contacts in the stolen lists (which may include friends, family, business contacts, and professors) or use these contacts to send spam e-mails and/or malware in the name of the crook.

Why is your account important for crooks?

If you are asking yourselves why crooks take an interest in your e-mail accounts and harvest the e-mail addresses of your friends, the answer is simple. To send more spam.

Miscreants cannot register accounts automatically on webmail providers such as Yahoo, Google, Hotmail and the like because registrants need to fill in CAPTCHA. It takes time, and real people, to type the signs in. That, in turn, costs money. Stealing active accounts is a cost-effective way for an operator to automate attacks and, at the same time, allows them to read your contacts and get more victims.

What's to be done?

Log out from your e-mail accounts every time you're done reading or writing your e-mails.

Never click on links in spam e-mails.

Keep your antivirus and software updated.

###

For further information about Bitdefender, please contact

Marie-Claire Suter

Howorth Communications

(02) 8281 3815

Marie-Claire@howorth.com.au

Or

Rebecca Booth
Howorth Communications
(02) 8281 3225
Rebecca@howorth.com.au

About Bitdefender®

Bitdefender is the creator of one of the world's fastest and most effective lines of internationally certified internet security software. Since 2001, the company has been an industry pioneer, introducing and developing award-winning protection. Today, Bitdefender technology secures the digital experience of around 400 million home and corporate users across the globe.

Recently, Bitdefender won a series of important awards and accolades in the global security industry, including “Editor’s Choice” by PC Mag for Bitdefender Antivirus Plus 2013 and the “GoldAward” by TopTenREVIEWS that confirmed the software’s top spot among 25 tested security products. Bitdefender antivirus technology has also finished top in leading industry tests from both AV Test and AV-Comparatives. More information about Bitdefender's antivirus products is available from the company's security solutions press room. Additionally, Bitdefender publishes the HOTforSecurity blog, a sizzling blend of steamy computer security stories and stimulating visuals that spotlights the seedy underworld of internet fraud, scams, malicious software – and gossip.