



UNCLASSIFIED//FOR OFFICIAL USE ONLY



## 624TH OPERATION CENTER

INTELLIGENCE SURVEILLANCE & RECONNAISSANCE DIVISION

# Cyber Threat Bulletin

11 March 2011 (Issue 82)

Prepared/edited by 624 OC, ISRD

*\*The Cyber Threat Bulletin is designed to keep Air Force members knowledgeable of user & network threats. It is located on the AF Portal. It's against our policy to send out this bulletin or request personal data via email.\**

## MALVERTISEMENTS



sites as well. (Darkreading.com)

Social Networking is a huge part of society now and it is only getting larger. Most of us have at least one account on a social networking site (Facebook, Twitter, Myspace) if not all of them. One of the reasons for its popularity is that they are free use, but this is only possible because companies pay to advertise. These advertisements can often be exploited with malicious code so that when clicked on, your computer can become infected. Also to note, it's not just advertisements on these social sites that are problems. The links that users can post on their pages or the pages of other friends can direct unsuspecting traffic to malicious

Malvertising is on a significant rise, having doubled from Q3 to Q4 2010. Based on Q4 estimates, three million malvertising impressions were served per day, an increase of 100 percent over the year before, as compared to 1.5 million malvertising impressions. More than 1 million websites were estimated to be infected in Q4 2010. The probability that an average Internet user will hit an infected page after three months of Web browsing is 95 percent. (Darkreading.com)

So what can you do to keep yourself safe? Make sure you keep your firewall on, have a reputable antivirus software on your computer, and don't open any links you are not certain to be safe. Some antivirus softwares have a feature that can scan your facebook wall to check for any malicious links. Air Force members may now download home use antivirus software from a

UNCLASSIFIED//FOR OFFICIAL USE ONLY

non-mil computer, including a home computer, equipped with a CAC reader. Users can also contact their local help desk for a copy of home use antivirus software.



## PWN2OWN CONTEST



Pwn2Own is a computer hacking contest held at the annual CanSecWest security conference, beginning in 2007. Contestants are challenged to exploit specific software (especially web browsers and other web related software). Apple and Microsoft browsers were the first to be compromised in the Pwn2Own hacking contest at the CanSecWest security conference this year. French Security Company Vupen managed to hijack a fully patched 64-bit Mac OSX machine within 5 seconds of surfing to a site Vupen had rigged to upload a specially written exploit. The company found a flaw in WebKit, the rendering engine used by Safari, and specially crafted an exploit which bypassed both ASLR (Address Space Layout Randomization) and DEP (Data Execution Prevention) security technologies in the browser. Microsoft's Internet Explorer browser was successfully hacked by Metasploit developer Stephen Fewer. The Irish security researcher hacked into a 64-bit Windows 7 (SP1) machine running Internet Explorer 8 (IE8) using two different zero-day bugs in IE, plus a third flaw to jump out of the IE8 Protected mode sandbox. (ZDNet.co.uk)

*\*For any security related questions, issues, or concerns, contact your Unit Information Assurance Officer, Wing Cyber Surety Office and/or the Information Protection Office.\**

*Do you have a question, comment, or concern? Have a topic you would like to see in a future bulletin? Feel free to call us at DSN: 969-9612, or e-mail us at [624oc.isrd@lackland.af.mil](mailto:624oc.isrd@lackland.af.mil)*

*To receive automatic notification of each new Cyber Threat Bulletin loaded to the AF Portal, select the "Set an Alert" button at the top of the Cyber Threat Bulletin page. The Cyber Threat Bulletin is now available on the Community of Practice Air Force Knowledge Now 624 Operations Center ISRD Page.*