

'Police Ransomware' becomes Java 0-Day-Borne

SYDNEY/AUCKLAND– January 16, 2012 – The recently discovered vulnerability disclosed last week on Thursday has been finally patched by Oracle, but exploitation continues on computers that have not been updated.

Exploitation code is included in the world's most frequently used exploit packs such as BlackHole, Nuclear Pack and the Cool Exploit Kit, resulting in cyber-criminals taking advantage of the huge pool of vulnerable computers by planting ransomware.

Bitdefender has identified multiple campaigns that use the CVE-2013-0422 bug in Java to infect client machines with the notorious IcePol (also known as Reveton). Once the computer is successfully infected, the user is denied access to the desktop until payment of a ransom, which the criminals call a 'fine'.

Most of these attacks are directed from servers in the UK, Canada and the US but this doesn't mean that Australia is safe. We ranked 14th in terms of countries being affected by the exploit, with 0.87 per cent of the total number of incidents worldwide involving the exploit taking place in Australia. The Reveton ransomware has localised in multiple languages using IP addresses of the infected computers, and victims are spreading across the world. All it takes is a vulnerable version of Java.

Bitdefender also offers a free removal tool for computer users who don't have a Bitdefender product and have already been infected with the IcePol ransomware. The tool is available immediately via the Bitdefender Toolbox. Bitdefender customers have always been protected since the emergence of the threat by multiple layers of defense, from page blocks to signatures on the exploit files.

To stay safe, Bitdefender recommends consumers patch their Java distribution immediately to Update 11. Bitdefender also advises that users disable the Java plugin in the browser they are using for web-related tasks and only enable it in an alternative browser to be used for tasks requiring Java.

###

For further information about Bitdefender, please contact

Danielle Zhu

Howorth Communications

02 8437 5342

Danielle@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.