## iDefense Press Release:

# Exploitation for Unpatched Internet Explorer 7 Vulnerability in the Wild

**Dec. 10, 2008**

**Summary:**

On Dec. 9, 2008, security researchers found a previously unknown vulnerability in Microsoft Corp.'s Internet Explorer 7.0 being exploited in the wild. This exploit has already been incorporated into Chinese exploit toolkits and is actively being used to install information-stealing Trojans that target online games. No patch for the vulnerability is available at this time nor has Microsoft issued a public acknowledgement of this issue so far.

**Timeline of Events:**

- Monday, Dec. 8, 2008
- 03:48 - Approximate time the IE-7 Zero-Day Downloader Trojan first appears in China.
- Tuesday, Dec. 9, 2008
- 07:48 - McAfee, Inc. Announces "Downloader Trojan Exploits Hole in IE-7," reporting existence in China and effect on all versions of IE-7.
- 09:00 - iDefense Chinese expert finds copy of exploit code for analysis.
- 13:43 – iDefense publishes Initial Threat report (internal document ID# 477747).
- 15:00 - iDefense Daily Intelligence meeting Zero-Day status update.
- 16:00 - Microsoft Tuesday Post Release Summary meeting - Details and assignments coordinated for Early Assessment Briefing.
- 19:00 - iDefense Patch Tuesday Early Assessment Briefing Call. iDefense analyst reports: All IE7 versions effected; exploited in the wild; Posted on a Chinese forum by Graysign; an XML Tag issue associated with mishandling of duplicate tag ID; mitigation - turn off scripting; Detection - currently, scanning for "dadong" would work.
- 21:28 - iDefense analyst finds a variant of the IE-7 Zero-Day. It is the same vulnerability with a different obfuscation method.
- Wednesday, Dec. 10, 2008
- 10:39 - iDefense creates vulnerability report (internal document ID#477806).
- 11:29 - Updated Threat report severity to HIGH to reflect confirmation of exploitation against fully patched systems.
- 11:36 - iDefense analyst added the exploit from Milw0rm to Vulnerability report.
- 12:22 – Shadowserver publishes a list of exploit sites in the wild (http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20081210)

**Facts:**

- The Chinese *knownsec* security team released an advisory on Dec. 9, in which they acknowledge that the exploit code was leaked by one of their members (http://www.scanw.com/blog/archives/303). According to their notes, they had mistakenly assumed this issue to be for an already patched vulnerability.

- According to *knownsec*, earlier this year a rumor emerged in the Chinese underground about an IE7 vulnerability and in October it began to be trade privately. In November it got into underground black market and was traded for about $15K. Later in December, it

emerged and people sold the exploit second or third hand for about $650. Finally, someone purchased those second hand exploits to develop and deploy a Chinese gaming Trojan.

**iDefense Quotes:**

"The IE 7 Zero-Day is really nasty. No patch. Mitigation options are not good; some are draconian. Dig in folks, this could be a rough ride."

-- Rick Howard, Director of Intelligence, iDefense Security Intelligence Services (rhoward@idefense.com)