

By [Mariusz 2007](#), Technology News Editor

[284 Days - The Attack Window of IE in 2006](#)

Version 6

An attack window is defined as the period of time between the availability of a zero-day vulnerability and the moment the vendor produces a security update addressing the flaw. During this time, users are exposed to exploits and have no defense barrier against attacks. [Brian Krebs](#) over at Washington Post has compiled statistics that reveal the attack window associated with Internet Explorer 6 in the past year. Microsoft's Internet Explorer is the dominant presence on the global browser market with a share of approximately 80%, according to data made public by Market Share by Net Applications. In this context, IE users have been exposed to attacks for a total of 284 days in 2007. "There were at least 98 days last year in which no software fixes from Microsoft were available to fix IE flaws that criminals were actively using to steal personal and financial data from users. Microsoft labels software vulnerabilities "critical" -- its most severe rating -- if the flaws could be exploited to criminal advantage without any action on the part of the user, or by merely convincing an IE user to click on a link, visit a malicious Web site, or open a specially crafted e-mail or e-mail attachment," explained Krebs. Krebs informed that for 284 days in the past year, Proof-of-Concept and exploit code impacting either zero-day or unpatched critical vulnerabilities in Internet Explorer was available in the wild. Although Microsoft has delivered Internet Explorer 7 on October 18, 2006, the latest Microsoft browser has not enjoyed an adoption rate that would take Internet Explorer 6 out of the equation. In fact, analytics company OneStat revealed that on November 6, 2006, the global usage share of IE7 was of just 3.06%.