Holiday season is fertile ground for most malware infections

Research data compiled by the site over the last year (late 2010 to present) showed Dec. 27, 2010, to have the largest spike in malware infections it tracked, with a 56% increase over the previous day. SpywareRemove.com is a malware tracking website that is owned and operated by security firm Enigma software.

The company believes the Dec. 27 date was prolific among cybercriminals due to the after Christmas rush of gift exchange and post-holiday deals by retailers. The website compiled its list of the top five malware infection dates according to its tracking data:

- Dec. 27, 2010
- February 27, 2011 (malware and phishing attacks attributed to the New Zealand earthquake)
- March 28, 2011 (breaking news of the Arab Spring protests)
- April 4, 2011 (the Monday after April Fool’s day)
- Nov. 28, 2011 (Cyber Monday)

"The number of infections we track fluctuates a lot depending on internet traffic", noted Alvin Estevez, CEO of Enigma Software and editor of SpywareRemove.com. The firm’s chief executive said malware infections dropped precipitously on Thanksgiving – to a yearly low – which is to be expected with many internet users in the US taking time to visit with family. "But as soon as Thanksgiving was over, the traffic – and the infections – shot up again...on Black Friday, all through the weekend, and hit a peak on Cyber Monday, up 28% from Thanksgiving Day’s low."

What the top five malware infection dates indicate, said Enigma, is that malware writers use a two-pronged strategy to deliver their malicious payloads to computers by taking advantage of one-time major events, as well as fixed dates on the calendar during the holiday season.

"The bad guys know that lots of people will be scouring the internet for good deals and the hottest holiday items", Estevez continued. "And they've populated the internet with phony web sites and links that trick folks into downloading spyware."

Why Not Watch?
Related to This Story

- Red October cyber-espionage campaign used highly sophisticated infiltration techniques
- Korean info-stealing malware targets Russian space, telecom targets
- Fortinet expert warns on mobile malware that encrypts its data streams
Christmas/New Year malware saw a surge of themed malware attacks.