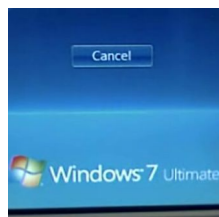


27 March 2008

By: Marius Oiaga, Technology News Editor

Windows 7
ThinkNext

[Whatever You Do, Do Not Download XP SP3 and Windows 7 from Torrent Trackers](#)

Or anything else for that matter

Whatever you do, do not download [Windows XP Service Pack 3](#) and Windows 7 from torrent trackers. Or anything else for that matter. Users that are looking for a free ride via peer-to-peer networks are at risk of getting a tad more than they bargained for, explained Billy McCourt, SophosLabs Security Researcher. McCourt explained that one area of malicious code research involves crawling the Internet in search for malware samples. "One of the simplest ways the bad guys can try and distribute their malware is by using P2P networks. P2P networks such as KaZaA and Gnutella are file sharing systems and typically host, possibly illegal, copies of MP3s, films and software. These networks might seem like an odd choice to spend time researching since the primary users of these networks are probably under the age of 14. The point is that they are simply a distribution system and the chances are high that malware found on these networks will also appear in other locations. P2P networks are also relatively easy to crawl," [McCourt explained](#). Shortly after the first details were leaked about the successor of Windows Vista, [Windows 7](#) in January 2008, various downloads began popping out on torrent and warez websites masquerading as the first taste of the next Windows client from Microsoft. It was never confirmed that the actual Windows 7 bits had been leaked, and in this context, users could have downloaded just about everything, including malicious code. A more recent example involved [Windows XP SP3 RC2 Build 5503](#). This was a private development milestone from the Redmond company that got leaked, and made its way onto torrent trackers being advertised as the RTM build of the third and last service pack for XP. At that time, Microsoft warned against downloading code from third-party sources citing security reasons. According to Sophos, Microsoft was right to be concerned. "Within a P2P client we did some keygen related searches. Keygens (key generators) are programs that generate valid serial numbers / registration codes for applications so they are basically used by software pirates. A couple of searches we carried out were: Sophos keygen and Linux keygen. These are ridiculous searches since no Sophos product uses this type of registration model and Linux certainly doesn't! They did however turn up some (not so unexpected) results: Troj/Agent-GGQ; PlayMP3z Installer and Troj/Agent-GFL (twice)," McCourt added. Windows XP Service Pack 3 Release Candidate 2 Refresh can be downloaded from [here](#).