

19 August 2006

By: Marius Oiaga, Technology News Editor



Windows Vista Inherits the Sins of the Father

And shares migratory vulnerabilities with its predecessors

In all fairness, Windows Vista has no Father Program, but it does have predecessors. A short heritage line; feeble, weak lived variations, with the exception of XP and a genealogy plagued by vulnerabilities make up Vista's background. But the big question here is what will happen to Vista once it is thrown out of Microsoft's Garden of Eden. The operating system will be the most prized item of prey on the World Wide Web. And in this regard, Microsoft's Security Scripture proved to be a picaresque prophylaxis at best, an aspect of Vista's strategy taken in vain. Vista's repeated delays only fueled the appetite of those on perennial hunt, a perpetual starvation status for a suitable candidate. And Microsoft has built up a paroxysm of hunger following public exhibitions of Vista Beta 2 at Hack in the Box in Kuala Lumpur and at Black Hat in Las Vegas. The leaps of faith Microsoft took with security displays during the products development stage caused a momentum of conversant, accrual and intimate connections converging on Vista. Recently, Ballmer prophesized a moderate and incrementally divided basis for the development of the operating systems succeeding Vista, rather than mammoth updates. Microsoft's CEO, casting verbal stones at Vista's source of all evils, the simultaneous implementation and integration of multiple innovative features, swore off the company's tactics to evolve its OS on the wake of Microsoft's decentralization efforts, generalization of core businesses, and multicore strategy. Symantec presented a trilogy report following a generalized evaluation of the operating system's network stack, User Account Control (UAC) technology and kernel mode security and stated an instability diagnosis concluding that Vista will deliver an inferior level of protection compared to its predecessor. And Symantec is not a singular case in this regard; security experts from Agnitum have pointed the finger at Microsoft for eliminating third party proactive protection by denying kernel control via the altering of the Service Dispatch Table, through the implementation of Kernel Patch Protection. Expert Joanna Rutkowska from the Singapore-based firm COSEINC demonstrated at the Black Hat conference in Las Vegas a method of circumventing Vista's integrity checking panoply. Through a virtualization tool bypass Rutkowska interfered with the management process of loading unassigned code into Vista's kernel, while the OS was running in administrator mode, and installed a rootkit. 918899 and 917422 are two cumulative Windows related vulnerabilities patched by Microsoft on August 8. But, while initially the Redmond Company has left its latest OS out, product manager Alex Heaton confirmed that the vulnerabilities have migrated to Windows Vista and that the company has made fixes available via Microsoft Download Center. The software giant has set a precedent by offering security updates support for a product while in beta phase and the company saw a decent amount of criticism related to the issue. The actual volume of patches made available by Microsoft for Windows Vista Beta 2 is a perspective that delivers assurance of the company's continuity with the patching process, following the final release of the OS. Microsoft has issued security bulletins to address the vulnerability in Vista's kernel and the cumulative security flaws related to its Internet browser that performed a migratory transition from XP to Vista. Heaton informed that the support will be ceased concomitantly with Release Candidate 1. The sins of the father... Microsoft's incubatory exorcism failed, Vista vulnerabilities proved inherent to the system, a collateral baggage of the code source genealogy.