
future derivatives

Posted by Ima Ufo - 2010/01/07 14:27

By Joe Wilcox of oddiytogether.com. There are many measures of success, and some are less desirable than others. Windows is the standard by which cybercriminals measure their wares—eh, malware. Their devotion to Windows is testament to Microsoft's success. The company should just accept the faint praise for what it is. Microsoft claims that Windows is more widely attacked by malware than, say, Mac OS X because of volume; many, many more people use Windows PCs than Macs. The claim is great PR, because it kind of makes sense and is unprovable without Macs gaining lots more marketshare. But on closer examination, the claim is pure BS. Microsoft security experts know so, or they're delusional. Malware writers go where the money is, just like bank robbers of an earlier era. For years, Mac defenders have argued that Mac OS X was much more secure than Windows. That its architecture was more hardened to attack—analogue to a bank with better security systems and hardened vault. I've made the same claim, too. But Windows Vista and successor 7 tighten up administration rights so that they're closer to Mac OS X security. Also, Mac OS X has yet to be tested the way Windows has. There wasn't enough money in it for malware writers, and, again, that has little to do with Windows' greater adoption. I've long asserted that Windows succeeded because it allowed so many third parties to make money. It's one of attributes of successful platforms:

- * They have at least one killer application people really want
- * Tools and APIs make good applications easy to develop
- * Platform provides plenty of really useful applications
- * Third parties make lots of money

The fourth attribute is the most important, and it's fundamentally reason why Microsoft eclipsed Apple in the late 1980s and 1990s. By controlling the hardware and not licensing the software, Apple limited how many partners could make how much money off the Macintosh platform. By comparison, Windows offered seemingly limitless opportunities. Windows was a gold rush for business adopters, component manufacturers and suppliers, PC OEMs, peripheral manufacturers, resellers, retailers, software developers, software distributors and system builders, among others. Victim of Its Own Success Microsoft describes this community of moneymakers the Windows ecosystem. That's an apt description, with natural overtones. Wikipedia, citing RW Christopherson, *Geosystems: An Introduction to Physical Geography*, Prentice Hall 1996, describes: An ecosystem is a natural unit consisting of all plants, animals and micro-organisms (biotic factors) in an area functioning together with all of the physical (abiotic) factors of the environment. An ecosystem is a unit of interdependent organisms which share the same habitat. Ecosystems usually form a number of food webs which show the interdependence of the organisms within the ecosystem. Microsoft's Windows platform fits the definition in an economic sense, with money substituted for "food webs." These independent organisms feed off the money opportunities exposed by the Windows platform. I wasn't a computer nerd in school. But I was a science geek, and biology was my primary field of study at a time when schools discouraged the major. I've got pretty good sense about how biological systems work—well, good enough for this post. Within natural ecosystems, some organisms feed off—in human terms, exploit—others. Microsoft talks about the Windows ecosystem in context of the aforementioned "good" partners. But there is a shadow ecosystem, too, of so-called cybercriminals and malware writers who profit for many of the same reasons as hardware manufacturers, retailers or software developers. Some of these Windows ecosystem organisms are parasites. In nature, many parasites serve important roles. Can the same be said for computing? Absolutely. Within the human gut are bugs necessary to digestion. There are members of the shadow ecosystem that profit from fixing security bugs rather than exploiting them; their assistance is vital to Microsoft and its customers and partners. But many of these parasites and other organisms are hostile. They attack the Windows ecosystem and would destroy it by profiting from it. Microsoft can't escape the shadow ecosystem. The ecosystem of developers, resellers and other partners make money from Windows platform strengths. The shadow ecosystem profits from the platform's weaknesses. Ecosystems Must be Managed I'm surprised that Microsoft's math-oriented cyberfighters don't apply more science to shrinking the shadow ecosystem. Many environmentalists and some politicians propagate amazing folklore that natural systems should be allowed to run amok. That it's wrong to interfere with natural systems. Bullshit. Natural systems tend to thrive when they are carefully, but not too aggressively managed. Human beings are part of the natural ecosystem and have a role, too. Human beings' role is far more important and obvious for the ecosystems they create for themselves. For example, financial systems are ecosystems, too. In the aftermath of the econolypse, economists, politicians and other experts are concluding there wasn't enough regulation (e.g., management) to maintain balance. The government played a role, by lowering interest rates so far that they became fertilizer for destructive weeds (credit/debt and other derivatives) that overwhelmed the financial ecosystem. The treasure of valuable foodstuffs that many people thought they had procured during the boom turned out to be nothing but valueless weeds in the bust. Natural ecosystems could teach Microsoft something about security. Microsoft is fairly aggressive about managing the larger Windows ecosystem, but needs to better manage the shadow ecosystem and reduce its numbers. The monthly security patches is good management practice. People tend to forget that, aside from zero-day exploits, Microsoft acts proactively. The releases are security due diligence. Last week's beta release of Security Essentials is another good move. I'm on the beta and will report about using the software sometime soon. But security software is a reactive solution. Microsoft needs to be even more proactive, and monthly patches don't go far enough. Sure, Microsoft deserves praise for proactively undertaking its managed code initiative and making security analysis a fundamental and vital part of software development. Given this post is already so long, I'll save proactive suggestions for the future. The American Chestnut Metaphor To reiterate, Microsoft cannot avoid the shadow ecosystem. It's a natural byproduct of the broader Windows ecosystem. But Microsoft can better manage—and even reduce—the risks. Every ecosystem is susceptible to devastation. The shadow ecosystem can do more than just release malware, which steal personal identities or account information for auctioning on eBay-like black markets (there's even trade in viruses). If not properly managed—or contained—the shadow ecosystem can become a fungus capable of devastating the broader

Windows ecosystem. For North America, the greatest environmental tragedy of the Twentieth Century wasn't the increase of global emissions but the mass destruction of a thriving and vital natural ecosystem. In 1903-04, the Bronx Zoo imported Chinese Chestnut trees for display. A deadly fungus infected the imported trees; the American Chestnut had no natural defense. The Chestnut was a popular fixture in Nineteenth Century but not Twentieth Century literature for a reason. In many locales along the North American Eastern seaboard, the Chestnut was one in four trees; there were whole groves in the Appalachians. Within three decades, the blight killed 90 percent of the Chestnut trees in North America. The Chestnut all but disappeared from the American landscape. The tree's demise devastated timbering, tannin and other industries. Huge populations of wildlife diminished because they lost food supply. For example, wild turkeys declined more because of the Chestnut's loss than from the intrusion of humans into their habitats. How many habitats and industries would be lost if the Windows ecosystem were similarly and suddenly devastated?

=====