

## RE: Trend Micro's Vista "0day exploit auction" claim

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-12/msg00348.html>

---

- *From:* Simple Nomad <[thegnome@xxxxxxxx](mailto:thegnome@xxxxxxxx)>
  - *Date:* Wed, 20 Dec 2006 16:16:37 -0600
- 

On Tue, 2006-12-19 at 21:55 -0500, Roger A. Grimes wrote:

I can't verify it. But \$50K for an exploit against an OS that will not be widely deployed for many months seems to be excessive. Who in their right mind would want to pay \$50K to exploit 10 machines before the exploit is captured, sent to MS, and patched, all before the general population really starts running it.

It doesn't pass the commonsense test to me. A zero day on XP Pro would be oh, so much more valuable.

XP exploits *\*are\** more valuable. Considering XP exploits already go for as much as twice that, \$50k actually seems reasonable, or if not reasonable, at least what the market will bear. I haven't seen auction boards recently (in fact since fed crackdowns it is getting harder to get on some boards) and never saw Vista on there as it was before Vista's time, but I have seen large amounts. While up to 6 figures for a remote root XP exploit seems excessive, \$50k for Vista does not strike me as outrageous, all things considered.

Organized cybercrime, for lack of a better word, seems to be fairly well organized. An aggressive business person is willing to spend money to make money, so having multiple 0days for future business expansion would only make sense, particularly in an area with so much unlaundered cash floating around. If the ecommerce sites start moving to Vista and you have remote root on Vista, burning a 0day to hit a few dozen major sites and grab customer lists, CC #'s, etc is totally worth \$50k.

Another thing to bear in mind is that some of the value here may lie in something besides actual money. For example someone might be willing to trade a run of CC #'s for a Firefox exploit, and if each credit card would normally fetch \$200, your exploit might be worth 50 credit card numbers which have a street value of \$10k. If you were real good at carding you could easily turn this into twice or three times that. Otherwise the exploit might only be worth a couple thousand in actual cash.

RE: Trend Micro's Vista "0day exploit auction" claim

-SN