Another interesting detail from the analysis of Windows Error Reporting data for Explorer

devblogs.microsoft.com/oldnewthing/20080521-00

May 21, 2008

Raymond Chen

I was in a meeting last year where I learned an interesting tidbit of information. One of the people at the meeting was looking at the error reports submitted against Explorer, and the breakdown went something like this. For the purpose of discussion, the number of reports have been normalized into “units”, the precise meaning of which is left unspecified, but is meaningful for comparison purposes.†

Rank	Cause	Units
1	XYZ.v2 Virus	6 million
2	XYZ.v3 Virus	5.5 million
3	XYZ.v1 Virus	5 million
4	XYZ.v1 Virus	4.5 million
5	XYZ.v2 Virus	4.5 million
6	XYZ.v2 Virus	4 million
7	Bug 271828	50,000

The XYZ virus (not its real name) and its variants together are responsible for the top six categories of Explorer crashes, and by an enormous margin. Seventh place, an actual bug, comes in at only 1/80th the rate of number six; if you group all the XYZ virus failures together, then the combined virus failures outnumber the most popular Explorer bug by a factor of nearly 600. I remember reading a report that half of Explorer crashes can be directly attributable to malware. Seeing the top Explorer crash swamped by a single virus really drives that point home.‡ **Footnotes** †I don’t know what these units mean either.

‡The anti-malware team is very interested in this data, because when a new category of Windows crashes suddenly spikes in popularity, there’s a decent chance that a new virus is on the loose.

Raymond Chen

Follow