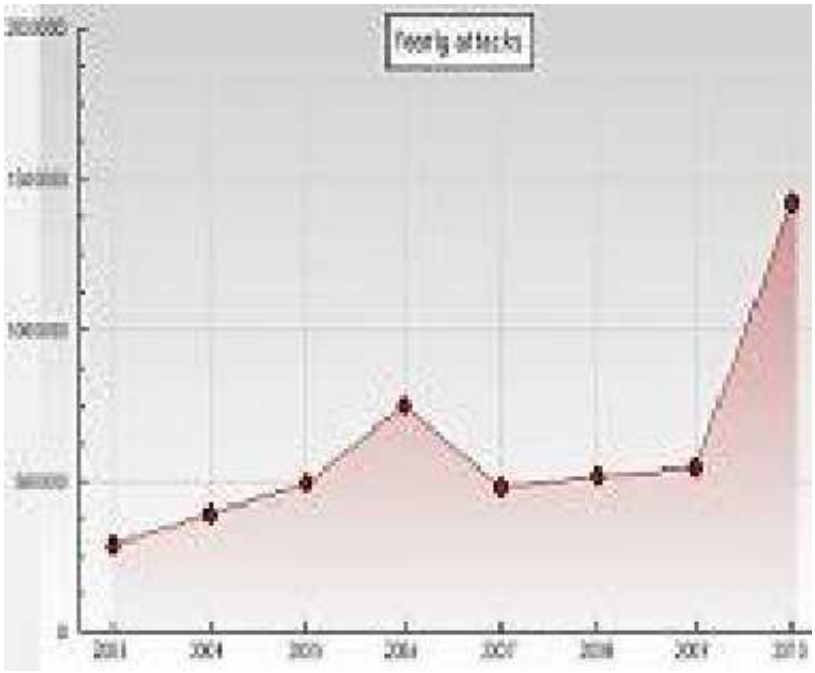
Defacements Statistics 2010

2012-01-12 15:34:18 by Southern

Almost 1,5 million websites defaced, what's happening?

Marcelo Almeida (Vympel), Boris Mutina (Minor)



Last year the Zone-H archived a sad record number, we archived 1.419.203 websites defacements.

Why and how this is happening?

If you are looking at on the stats, the things remain the same: file inclusion, sql injection, webdav attacks and shares misconfiguration are still at the top ranks of the attack methods used by the defacers to gain first access into the server. As an important factor influencing the stats we consider the fact that last year brought a very high number of the local linux kernel exploits.

Since many years ago, Linux became the most used OS for webservers and of course the preferred target for the defacers. Last year we archived 1.126.987 attacks against websites running on the Linux systems. The most used exploit by the defacers is the CVE-2010—3301,that was fixed in 2007 and was mysteriously reintroduced in 2008, in a large pile of kernel versions x86_64.

But should be the out-of-date Linux server the only reason of this huge amount of defacements?

Yes and no.

We were talking about local kernel exploits, but the first problem is in the website code. For example, we received too many single defacements due a remote upload flaw in OsCommerce CMS, that allows the defacers to upload anything to the CMS folder without a proper credential check. When this flaw became public, the developers had a too much time to fix it, but the fix appeared few months later. Pity.

Year after year, the developers are still coding by an unsafely, keeping tons of the remote and local file inclusion and the SQL injections, that the attackers use as the first step to gain the access into the server OS.

Then an another problem with the out-of-date system is that the old kernel versions indicate also that another packages (sometimes also misconfigured) by performing privilege escalation for the services/users access.

But we should not speak only about the Linux servers, the Windows Servers are also in the stats, (not) surprisingly still hacked by the same flaws like in year 2000 and early. Every year we also recorded a high number of the webdav and shares misconfiguration attacks. For webdav there are tons of the updates, for shares too, administrators just need to put their hands on it and update and/or change the configuration.

From the results one outcome is clear—code developer teams and webserver admins are still living in two distinct worlds. And if something is not working properly, their answer is that this is most likely the other side’s fault. While this “fight” continues, the defacement count still grows up.

If you have any comments, send them to comments@zone-h.org

Zone-H
http://www.southernwolf.net//modules.php?name=News&file=article&sid=3541