German Spam...Maybe?

By *srlinuxx*
Created *15/05/2005 - 1:42pm*
Submitted by srlinuxx on Sunday 15th of May 2005 01:42:26 PM Filed under Security [1]

Since taking over as handler on duty, I have had a perplexing question that I am trying to understand. Somehow in the past 4-5 hours (as of 5am UTC), I have received a number of "German spams". Getting spam is not an overly out of the ordinary thing for me as I do sift through many mailing lists and work email address aliases that are published on websites here and there. However, I do not remember the last time I had a German Spam show up in my inbox. Chinese, or other Southeast Asian spams do happen some, but I would suspect that English is the primary type of spam we all see.

Well the thing that has struck me is that several of my accounts have now received maybe 15 or 20 different German spams. Each message involves a different set of URLs and has URL(s) to various German news are personal editorial sites (I think).

My real question is whether or not something odd on the web pages people may be clicking on or in the email? So far I do not see anything odd (like IFRAME junk or similar.) So is there a piece of malware that is being used to relay this junk. I suspect so. But what is it? No clue. Is there any other motives other then to spam it out? I don't see a money trail, but that does not mean it is not there.

So to our readers, has anyone else seen a sudden influx of what might outwardly look like German Spam, that may actually have some actual interesting security connections that we need to be aware of before Monday gets here?

Any of you know of a new piece of malware that might be causing some of this, or perhaps old botnet machines being used as spam proxies suddenly?

Updated 13:00 UTC --

It would appear that this may be related to the Sober.Q virus per
http://www.viruslist.com/en/weblog

Thanks to everyone that responded this morning (overnight for me) with comments and reports of seeing the same thing that I was.

Source [2].

Security

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] http://isc.sans.org/