TECHNICAL SERVICE BULLETIN (TSB)

NVIDIA Timeout

ComSifter®

protect web users now!

TSB Date: March 28, 2012

IN THIS DOCUMENT

- Scenario
- Resolution
- Summary
  What can you do?

SCENARIO

The customer called Comsift Technical Support, complaining about load warnings and extremely slow—and sometimes corrupt—Access Log data. At the request of Comsift Technical Support, the customer analyzed the number of total connects shown in the Top Sites Report (`Admin > System Logs > Top Sites Report`). The Top Sites Report showed over 1.1 million connects to the Internet over the past seven (7) days. The customer informed Comsift Technical Support that they had a small network, with 30–60 computers online throughout a typical day. A connect is what is used by the client browser to fetch objects from the Internet. A single, typical page view can contain from one (1) to many hundreds of connects.

The question then became, ***"What is causing this phenomenally large number of connects from a relatively small network?"***

RESOLUTION

Upon further review the customer noticed that `nvidia.com` had risen to the top of the Top Sites Report with over 900,000 connects. The second entry in the Top sites was only 30,000 connects. The customer then did a search for `nvidia.com` in the Access Log and quickly determined that a large number of entries were coming from a new computer that was unable to update an NVIDIA graphics card driver. The customer noted that at one point there were 90 entries per second from this one computer. The customer added the `nvidia.com` domain to their Full Exception Domain List (`Filter Setup > Master Filter > Full Exception Domain List`) allowing the computer to download the necessary driver. Within one day, the number of connects dropped from over one million to half of that—more in line with what would be expected for the size of the customers network.

SUMMARY

In the past, Comsift has seen computers with malware and poorly written "phone home" programs/applications generate the equivalent of an internal Denial of Service (DOS) attack. This has never before been seen with a mainstream company.

What can you do?

The Top Sites report was designed to give you a quick look at your network. Networks are surprisingly stable. If you watch your Top Sites Report, you will notice that the Top Five sites seldom change and the number of connects becomes stable within a +/– 20% range.

If you see a large abrupt change in your Top Sites or the total number of connects, it is an indication that further analysis is warranted. As our customer did in this case, try searching the Access Log with the Top Sites entry and see if the connects are coming from a small number of computers (possibly indicating a problem) or from the whole network (indicating something new in the network users daily regimen).