Evan Cruz

B00320293

Assignment 1

CSCI4171

The internet is widely available in all parts of the world at all times. However, countries have tried to have censorship on the internet causing internet traffic to decrease in these areas. Natural disasters have also caused changes in internet traffic. Internet Background Radiation (IBR) is unsolicited traffic on the internet that is sent out without user input. Using IBR and other techniques, Caida was able to analyze how events, specifically censorship and earthquakes, effect the internet traffic in the affected area. Two countries in particular were studied due to their heavy censorship. The countries studied were Egypt and Libya who were chosen due to their governments fully shutting down the internet due to protests. Two natural disasters were also studied. These disasters were earthquakes in New Zealand and Japan. IBR does offer many advantages and uses in analysis, but there also drawbacks to the use of IBR. Caida hopes that their use of IBR will allow them to better study the effects of censorship and natural disasters.

IBR is unsolicited one-way network traffic that is sent to random IP addresses. IBR is usually either malicious (worms or scanning for network vulnerabilities) or inadvertent behavior. IBR has been used for a number of years to study malware characteristics. In the study produced by Caida the IBR traffic from affected countries are monitored to, not study malware, but instead study the way that internet traffic is affected. They also did this to show the characteristics of the events and impact on communication. IBR has three main causes. The first being backscatter from DoS attacks, the second being scans for network vulnerabilities or for other reasons, and the last being from bugs or misconfiguration. Backscatter is the response packets sent to the source IP trying to create a DoS attack. Since the IP address of DoS attackers are usually spoofed, the response packets go nowhere and are thus captured by IBR telescopes. Scans also are captured since they may scan for non-existing IP addresses randomly or through assigned scans. Finally, misconfigured systems can create IBR by setting an incorrect IP on a proxy server. IBR was used to study these effects because it does not require a user to directly do anything. Therefore data will be sent out automatically from machines outward to various destinations.

One of the first things that Caida studied was the outages that happened in Egypt. On January 27th, 2011 there were multiple reports of almost complete route withdrawal from routing tables. The internet outage was ordered by the Egyptian government in response to the protests that were happening at the time. In Libya, just days after the Egyptian outage, a very similar occurrence happened. A protest began and on February 18th, 2011 an outage was ordered in Libya. Using the USCD IBR telescope data was first collected from areas isolated to Egypt and Libya. The data was gathered covering a period over a number of days that both include outage days and non-outage days. During the non-outage days and outage days, the background radiation and the number of significant IPs followed similar graph lines. From February 2nd – February 4th the amount of backscatter from DoS attacks was significantly higher than normal. The network traffic had a large decrease when the internet ban was enforced on January 27th and returned to normal rates when it ended on February 2nd. IBR traffic remained during the outages as well likely due to the fact that some network prefixes would not be removed. Libya also displayed similar results with distinct IPs dropping to almost zero with the outage. The data studied here clearly shows that censorship is both possible and effective if governments decide to enact it.

Two earthquakes were then looked inspected by Caida. The first earthquake studied was one that struck New Zealand on February 22nd, 2011. The second earthquake studied was the one that struck Japan on March 11, 2011. The characteristics of each earthquake were inspected to determine any key differences between the two earthquakes and if it would affect the internet traffic differently. It was determined that the number of distinct IP addresses were higher in Japan due to the larger population and that the epicenter of the earthquake in Japan happened fairly far (100km) from any distinct IP address. The range of addresses affected varied in both places. Using an algorithm that Caida came up with, they determined a range of IPs from the epicentre of the earthquake. There was 20km of affected IPs in New Zealand and 300km of affected IPs in Japan. Using a geolocation service Caida was able to gather the effected IP addresses. Data was collected from a few weeks before the earthquake and after the earthquake. The IBR data was also collected during this period. The traffic is not zero and would likely never be zero because not all internet traffic would be halted by an earthquake. Another reason that the traffic would not be zero is because the geolocation service used by Caida cannot be expected to be 100% accurate. Some network traffic was also less affected by the earthquake which could be true or Caida had some errors in their analysis. The amount of unique IPs dropped significantly in both Japan and New Zealand when the earthquake happened compared to the normal rates. The earthquake in New Zealand however was much smaller than the one in Japan. This caused the internet usage rate to return to normal rates much quicker than in Japan. Also Japan had a much steeper drop in usage compared to New Zealand.

Despite many advantages that IBR offers, there are also a few drawbacks to this approach. The reliability of IBR is largely influenced by random and unpredictable events. It could be possible that a large botnet could be shut down by someone causing some IBR data to just stop. ISPs could also limit backscatter by stopping spoofed packets with fake IPs. Software patches can also prevent computers from emitting IBR by patching over software vulnerabilities. Some major disasters could also destroy computers thus requiring replacement of them, and causing IBR levels to be reduced. It is even possible that there is no IBR in an area at all, although the chances of that are incredibly low. The geolocation tools that they used are also relatively inaccurate. For New Zealand the accuracy was 62% and for Japan it was 69%, meaning there was a large amount of inaccurate data used in their studies. The one that Caida used however was about as accurate as other geolocation services.

Caida was able to determine the effect of geological events and internet censorship mainly by analyzing IBR. Since this traffic is so continuous, by looking at a large period of time it is possible to determine the short and long term effects of an event like censorship or an earthquake. Their findings showed that it would be easy to determine which countries or cities had lost internet connectivity. They also say that using IBR allows them to infer on what events are happening, such as packet based filtering, that other forms of analysis can't such a BGP. Censorship is very easy to see by using IBR, and bounds of the censorship are easy to find. IBR can also be used to determine the extent of earthquake damage by seeing where IBR data is normal. Caida also determined that there was a few limitations to their approach. For example, they did not distinguish the difference between loss of network activity due to power loss or loss due to network connectivity. They believe that they have only scratched the surface and can find out much more with better and more effective analysis.

Bibliography

Alberto Dainotti, Roman Ammann, Emile Aben, Kimberly Claffy. 2012. *Extracting Benefit from Harm: Using Malware Pollution to Analyze the Impact of Political and Geophysical Events on the Internet*. Caida.
http://www.caida.org/publications/papers/2012/extracting_benefit_from_harm/extracting_benefit_from_harm.pdf