Internet censorship revealed through the haze of malware pollution

March 7 2012

On a January evening in 2011, Egypt – with a population of 80 million, including 23 million Internet users – vanished from cyberspace after its government ordered an Internet blackout amidst anti-government protests that led to the ouster of Egyptian President Hosni Mubarak. The following month, the Libyan government, also under siege, imposed an Internet "curfew" before completely cutting off access for almost four days.

To help explain exactly how these governments disrupted the Internet, a team of scientists led by the Cooperative Association for Internet Data Analysis (CAIDA) at the University of California, San Diego conducted an analysis based largely on the drop in a specific subset of observable Internet traffic that is a residual product of malware. Many types of malicious software or network activity generate unsolicited traffic in attempting to compromise or infect vulnerable machines. This traffic "pollution" is commonly referred to as Internet background radiation (IBR) and is ubiquitously observable on most publicly accessible Internet links.

The analysis marks the first time that this malware-generated traffic pollution was used to analyze Internet censorship and/or network outages, and the researchers believe this novel methodology could be adopted on a wider scale to create an automated early warning system to help detect such Internet reachability problems in the future.

"We actually used something that's generally regarded as bad – traffic

pollution due to malware – for a beneficial purpose, specifically to improve our understanding of geopolitical censorship behavior," said K.C. Claffy, CAIDA's founder and principal investigator for the research, funded by the National Science Foundation (NSF) and the Department of Homeland Security (DHS).

Added Emile Aben, part of the research team and a system architect with the Reseaux IP Europeens Network Coordination Centre (RIPE NCC), an independent organization based in The Netherlands that supports the infrastructure of the Internet through technical coordination: "We believe that research such as this has security relevance and implications for every nation in the world."

Specifically, the research team – including scientists in Italy and The Netherlands – used UC San Diego's Network Telescope, which consists of a globally routed segment of Internet address space that carries almost no legitimate Internet traffic. Also known as a 'darknet' because this subset of addresses does not have any devices assigned to them, the UC San Diego network telescope collects what could be considered "garbage" of the Internet, such as traffic due to mistyped IP (Internet protocol) addresses, malicious scanning of address space by hackers looking for vulnerable targets, backscatter from random source DoS (denial of service) attacks, and the automated spread of malicious software, including botnet and worm activity. The team also used other multiple sources of large-scale data available to the academic community, such as global routing signaling information.

"Using a combination of this data allowed us to narrow down which forms of Internet access disruption were implemented in a given region over time, but the malware-induced traffic helped us uncover things that the other data did not reveal," said Alberto Dainotti, who recently joined CAIDA from the University of Napoli Federico II in Naples, Italy, and served as lead author of the study, called Analysis of Country-wide

Internet Outages Caused by Censorship. "Among other insights, we detected what we believe were the Gaddafi government's attempts to test a firewall to conduct higher precision host-based blocking while they were executing the coarser approach of router-based disconnection."

"On a larger scale, we were able to analyze how regimes go about bringing down an entire country's Internet infrastructure," said Aben.

From the Geopolitical to the Geophysical

CAIDA has also been exploring the impact of geophysically disruptive events, such as major earthquakes or other natural disasters, on Internet connectivity. Another recent study was described in a study called Extracting Benefit From Harm: Using Malware Pollution to Analyze Political and Geophysical Events, published in the January 2012 issue of the ACM SIGCOMM Computer Communication Review. In this study, Dainotti, Claffy, and Aben, along with Roman Amman from the Auckland University of Technology, in Auckland, New Zealand, showed how IBR traffic revealed aspects of not only the Egypt and Libya political uprisings, but also during the powerful earthquakes that struck Christchurch, New Zealand, in February 2011, and Tohoku, Japan one month later – the most powerful earthquake to ever hit that nation.

Dainotti acknowledges that this research is still preliminary, and the team has not explored any automated early warning functionality for natural disasters. But the earthquake study above explored metrics for effectively and efficiently gauging the impact of disasters on Internet infrastructure, based on the analysis of IBR activity from the affected region or regions.

The metric they experimented with to analyze the earthquakes captured a level-shift in the number of IP addresses reaching the observation point. It clearly showed that the Tohoku earthquake had much higher

impact on network infrastructure than the Christchurch earthquake (partly because there is much higher population density and thus Internet infrastructure density in Japan). The researchers also were able to compare the geographic extent, or radius, of the damage, and approximate restoration times based on when IBR traffic was again observable by the UC San Diego network telescope.

"Although we have only scratched the surface, we are convinced that IBR traffic is an important building block for comprehensive monitoring, analysis, and possibly even detection of events unrelated to the IBR itself," said Claffy, noting that CAIDA plans further study in this area. "We hope our methodology will be used to detect outages or similar macroscopically disruptive events in other geographic or topological regions."

Provided by University of California - San Diego