innovation & regulation chair

Orange
Ecole Polytechnique
TELECOM ParisTech

Conference in Paris
June 23rd, 2010

Security, Internet, and the prevention of spam: The Role of Internet Service Providers in Botnet Mitigation

Pr **Michel J.G. van Eeten**,
Professor of Public Administration in the School of Technology, Policy and Management,
Delft University of Technology

Botnets -networks of machines infected with malicious software- are widely regarded as a critical security threat. Pr Van Eeten investigates empirically the effects of country-level policy measures.

Botnets -networks of machines infected with malicious software- are widely regarded as a critical security threat. Measures that directly address the owners of the infected machine end users are useful, but have proven insufficient to reduce the overall problem. Recent studies have shifted attention to key intermediaries -most notably, Internet Service Providers (ISPs)- as control points for botnet activity. Surprisingly little empirical information is available to assess the claim that ISPs are an important control point, as well as related claims, for example, that large ISPs are worse cybercitizens than smaller ones. This paper is a first effort to go beyond generalized arguments by dissecting the diversity of ISP and the number of infected machines in their networks. As most of the current spam is sent through botnets, the origin of spam messages provides us with a proxy for detecting infected machines. Using a global dataset of 138 million unique IP addresses that connected to a spam trap in the period 2005-2008, we have analyzed in detail the geographic patterns, time trends, and differences at the level of countries and ISPs. This data underlines the key position of ISPs as intermediaries. For example, in our dataset just 10 ISPs account for around 30 percent of all unique IP addresses sending spam worldwide; 50 ISPs account for over half of all sources. For the first time, the patterns in infected machines are connected to other data, such as the size of the ISPs and the country in which they are located. Using bivariate and multivariate statistical approaches Pr Van Eeten investigates empirically the effects of country-level policy measures on the number of unique IP addresses sending spam at the ISP level. The data reveals wide differences between ISPs in the relative number of infected machines, sometimes up to three orders of magnitude. Whereas the overall number of infected machines is largely driven by the size of the user base, we also find limited evidence that public policies to improve cybersecurity have the desired mitigating effects. Our findings confirm some of the claims made in the research literature but refute others.