Understanding Politically Motivated Adversaries: Targeted Threats and Censorship Product Fingerprinting

Phillipa Gill, Stony Brook University

Politically motivated adversaries change the way we think of attacks on the Internet. Unlike conventional online adversaries, who are motivated by economic gain, politically motivated adversaries are motivated to gain and control access to information and are willing to expend time and money to achieve their goals. In this talk, I will discuss research that characterizes the level of sophistication of targeted malware attacks and techniques to fingerprint specific instances of filtering technology used to violate human rights.

Targeted attacks on civil society and non-governmental organizations have gone underreported despite the fact that these organizations have been shown to be frequent targets of these attacks. In my talk, I will shed light on targeted malware attacks faced by these organizations by presenting our study of malicious e-mails received by 10 civil society organizations (the majority of which are from groups related to China and Tibet issues) over a period of 4 years.

Our study highlights important properties of malware threats faced by these organizations with implications on how these organizations defend themselves and how we quantify these threats. We find that the technical sophistication of malware we observe is fairly low, with more effort placed on socially engineering the e-mail content. Based on this observation, we develop the Targeted Threat Index (TTI), a metric which incorporates both social engineering and technical sophistication when assessing the risk of malware threats. We demonstrate that this metric is more effective than simple technical sophistication for identifying malware threats with the highest potential to successfully compromise victims. We also discuss how education efforts focused on changing user behaviour can help prevent compromises.

In addition to time spent targeting attacks, politically motivated adversaries are also willing to spend considerable amounts of money to achieve their goals. This has led to the development of a $5 billion industry for censorship and surveillance products. Many of these products are dual-use, and can be used for legitimate network management, however, their installation in national-level ISPs to monitor dissidents and censor online communications represents a threat to human rights. With many of these products developed by Western countries, governments of the US, EU and Israel have all placed sanctions on their export to countries that will use them to violate human rights.

My talk will present technical methods we have developed to identify and confirm the use of specific filtering technologies around the world. The first method leverages a combination of network scanning to identify installations and in-country network measurements to confirm that products are indeed used for censorship. Using this method we are able to confirm the use of two different products in four different countries. The second method uses the fact that filtering products use common templates when generating block pages to enable a retrospective look at product usage. We apply this technique on five years of data from the OpenNet Initiative and are able to identify installations of products that were missed in prior (manual) analysis of the data.