ACM Ethics
The Official Site of the Association for Computing Machinery's Committee on Professional Ethics

Case: Malware Disruption

Using the Code: Malware Disruption

Rogue Services advertised its web hosting services as “cheap, guaranteed uptime, no matter what.” While some of Rogue’s clients were independent web-based retailers, the majority were focused on malware and spam. Several botnets used Rogue’s reliability guarantees to protect their command-and-control servers from take-down attempts. Spam and other fraudulent services leveraged Rogue for continuous delivery. Corrupted advertisements often linked to code hosted on Rogue to exploit browser vulnerabilities to infect machines with ransomware.

Despite repeated requests from major ISPs and international organizations, Rogue refused to intervene with these services, citing their “no matter what” pledge to their customers. Furthermore, international pressure from other governments failed to induce national-level intervention, as Rogue was based in a country whose laws did not adequately proscribe such hosting activities.

Ultimately, Rogue was forcibly taken offline through a coordinated effort from multiple security vendors working with several government organizations. This effort consisted of a targeted worm that spread through Rogue’s network. This denial-of-service attack successfully took Rogue’s machines offline, destroying much of the data stored with the ISP in the process. All of Rogue’s clients were affected. No other ISPs reported any impact from the worm, as it included mechanisms to limit its spread. As a result of this action, spam and botnet traffic immediately dropped significantly. In addition, new infections of several forms of ransomware ceased.

Analysis

Rogue’s actions include violations of several principles of the Code. By allowing for the hosting of malicious software, Rogue facilitated the harm caused by their clients, violating both Principles 1.1 and 1.2. Additionally, Rogue was complicit in violating Principle 2.8, as the ISP was aware that their machines were hosting code that caused infections that were clearly not authorized. Finally, Rogue failed to consider the public good, violating Principle 3.1.

From the perspective of the worm authors, this case highlights a key nuance of Principle 1.2. Given that the worm was designed with the specific intent of causing harm to Rogue’s systems, the authors were obligated to ensure the harm was ethically justified. The worm aimed to shut down web services that were clearly harmful and malicious in nature, the intent of the worm is consistent with the moral obligations identified in Principle 1.1. Additionally, the worm included mechanisms to limit itself solely to Rogue’s systems, thus demonstrating an attempt to minimize unintended harm. Rogue’s retailer clients could rightfully object to the deletion of their data, so a better solution would have included additional precautions to avoid this unintentional harm.

The worm also highlights the guidance in Principle 2.8. The worm clearly accessed Rogue's systems in ways that were not authorized, destroying data in the process. However, the goal of targeting malicious software demonstrates a compelling belief that the service disruption was consistent with the public good.

These cases studies are designed for educational purposes to illustrate how to apply the Code to analyze complex situations. All names, businesses, places, events, and incidents are fictitious and are not intended to refer to actual entities.
