2nd USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '09)

Boston, MA
April 21, 2009

PANEL: ETHICS IN BOTNET RESEARCH

Summarized by Ghulam Memon (gmemon@cs.uoregon.edu)

Panel Chair: Paul Royal, Georgia Tech Information Security Center Panelists: Aaron Burstein, Dave Dittrich, Thorsten Holz, Jose Nazario, and Vern Paxson

There were differing views among both panelists and audience about ethics in botnet research. Some suggested that as long as we follow the law we are on the right path to ethics. Others (specifically, Aaron Burstein) commented that the law does not necessarily guarantee ethics. It more likely sets a lower bar for ethical behavior.

However, it turns out that even following the law is not that simple, since laws have not kept up with the ever changing cyber-world. Although computer researchers often have the skills and knowledge to combat botnet threats, the law can impede them. Dave Dittrich said that had he followed regular procedure, going through a long chain of law enforcement officials, when he first started doing botnet research, the attackers may well have cleared their tracks before he'd gotten anything done.

Stefan Savage suggested that, in general, researchers conduct botnet research and then evaluate whether they have done something wrong. However, no one really thinks about the motivations behind the research. Thorsten Holz said his motivation is to understand how these networks operate and inform others about the threat. He is not in a position to commercialize his findings nor does he want to. Jose Nazario made similar comments but noticed that other people may try to commercialize the acquired knowledge.

Vern Paxson stressed that law enforcement is only a footnote. We as a community must have our own set of ethics, which we will use for our research; if any violation happens, we can point law enforcement towards that set. He hopes that this panel will encourage such discussions in the future.

Dave Dittrich mentioned that when he first started studying botnets, any kind of traffic monitoring was punishable under state law. He was saved because of a specific agreement that University of Washington had. Someone raised the point that if one knows about a crime and does not report it (a botnet in this case), he or she may be charged with a felony. Jose Nazario asked whether once we know there are flaws in a botnet, can we proactively exploit the flaws and disband the botnet?

The panel concluded after agreeing on the following: (1) We must develop our own set of ethics. (2) We must bor-

row some knowledge from criminology. (3) We must work with law and policy-makers. However, we must be aware that law-makers do not always respond to these issues with the same level of urgency as we do, so we must be prepared for black holes. (4) We must inform society about this menace as much as possible.