Initial post

by Ayo Adeniran - Monday, 8 April 2024, 4:40 PM
Number of replies: 1
Case: Malware Disruption

The case study analysed provided insight into an ethical dilemma involving Rogue Services, an internet service provider (ISP), and the actions taken to address the hosting of malicious content on their servers. Applying ethical frameworks such as the Code of Ethics and Professional Conduct from the Association for Computing Machinery's (ACM) Committee on Professional Ethics and the British Computer Society (BCS), helps in assessing the actions of the involved parties and their implications.

As highlighted in the analysis of the case study, 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.

Also, the BCS Code of Conduct emphasizes principles such as ensuring the public interest, prompting professional competence and maintaining integrity. In contrast, the actions of Rogue Services appear to violate these principles. Rogue's refusal to intervene despite knowledge of the harm caused to their clients contradicts the Principle 3 "Show what you know, learn what you don't (number 6)" of the BCS Code, which calls for professionals to consider the wider implications of the negligent action or inaction on society. By prioritizing profit and adhering strictly to their "no matter what" pledge, Rogue neglects its responsibility to prevent harm and promote the common good.

However, the intervention through a targeted worm also presents ethical concerns, albeit with justifications. While the worm authors may have acted with the intent to disrupt harmful services, their actions raise questions about unauthorized access and potential collateral damage. Notwithstanding, the design of the worm to limit its impact solely to Rogue's systems demonstrates a level of ethical consideration in mitigating unintended harm, aligning with the BCS principle of public interest, as well as ACM's principle 2.8 since they acted in the interest of the public good.

References

ACM code of ethics (2018) *ACM*. Available at: https://www.acm.org/

BCS Code of Conduct (2022) *BCS Code of Conduct*. Available at: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct

by Fabrice Wouche - Sunday, 12 May 2024, 3:55 AM
Dear Ayo Adeniran,

Your analysis of the case study involving Rogue Services and the ethical implications of their actions is insightful and comprehensive. You have effectively applied ethical frameworks such as the Code of Ethics and Professional Conduct from the Association for Computing Machinery's (ACM) Committee on Professional Ethics and the British Computer Society (BCS) to evaluate the actions of the involved parties and their consequences.

Your identification of Rogue's violations of the principles of the Code, such as facilitating the hosting of malicious software and failing to consider the public good, is well-supported and aligns with the ethical standards set by both ACM and BCS. Rogue Services' prioritization of profit over preventing harm and promoting the common good is indeed a significant ethical concern that reflects a lack of professional competence and integrity.

Furthermore, your analysis of the intervention through a targeted worm demonstrates a balanced consideration of the ethical concerns involved. The potential unauthorized access and collateral damage raised by the worm authors' actions are appropriately acknowledged. The design of the worm to limit its impact solely to Rogue's systems does indeed show a level of ethical consideration in mitigating unintended harm, which aligns with the principles of public interest outlined by the BCS and ACM's principle 2.8.

Overall, your analysis provides a comprehensive examination of the ethical implications in the case of Rogue Services and the intervention through a targeted worm. Your understanding and application of ethical frameworks are commendable, and your insights contribute significantly to the discussion of ethical considerations in the field of computing.

Thank you for sharing your perspective on this thought-provoking case study.