

Initial Post

Case: Malware Disruption

This case discusses Malware Disruption behavior's effects on legal, jurisdictional, and social aspects in the context of computing professionals

Due to their involvement in hosting and enabling malicious activities, such as the distribution of malware and the facilitation of spam, Rogue Services may face legal action. They could be held criminally responsible for helping to facilitate cybercrimes, depending on the jurisdiction. The case illustrates the difficulties of combating transnational cybercrime, as Rogue Services was headquartered in a country with lacking laws to address such hosting activities. This raises concerns regarding the efficacy of international legal collaboration in combating cybercrime. (ACM, N.D.)

The actions of Rogue Services had significant negative consequences for cybersecurity and the safety of society. The hosting of spam, spyware, malware, and ransomware contributed to the proliferation of cyber threats, which could result in financial losses, data breaches, and business disruptions. This case study emphasizes the value of credibility and reputation in the digital sphere.

Comparison of the case study with the BCS code:

1) **Integrity & Professional Competence:**

The actions of Rogue Services demonstrate an absence of professional competence and honesty. Hosting spam, viruses, malware, and ransomware violates the BCS Code of Conduct's expectations for the ethical conduct of computing professionals.

2) **Professional Duty:**

BCS: Professionals in the field of computing should uphold the reputation and ethics of their profession and report unethical behavior to the appropriate authorities. The actions of Rogue Services harm the reputation of the profession of computing by contributing to cyber threats and illicit activities.

3) The actions of Rogue Services are not in line with their stated commitment to professional development whereas to assure the highest quality of service, it is essential that computing professionals maintain their professional knowledge and skills per BCS

References:

ACM (N.D). ACM Ethics.

<https://ethics.acm.org/code-of-ethics/using-the-code/case-malware-disruption/> [Accessed 12 August 2023].

BCS (2022). BCS Code of Conduct.

<https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf> [Accessed 12 August 2023].

BCS (N.D.). BCS Code of Conduct.

<https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/> [Accessed 12 August 2023].