Initial Post

by Amit Pahuja - Thursday, 17 August 2023, 7:52 AM
Number of replies: 3

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].*

In reply to Amit Pahuja

Re: Initial Post

by Ashok Kumar Shanmugam - Monday, 21 August 2023, 4:02 AM

Greetings, Amit.
Thank you for your insightful insights.
Your astute examination of the case pertaining to Malware Disruption behaviour offers a thorough comprehension of its legal, jurisdictional, and societal ramifications. The investigation into the engagement of Rogue Services in illicit operations, such as the dissemination of malware and facilitation of spam, highlights the possible legal ramifications they may face. The user's comment on the potential criminal liability of those facilitating cybercrimes, according to jurisdiction, highlights the complex legal framework surrounding cybercriminal activity (ACM, N.D.).

The mention of Rogue Services' headquarters being located in a location with insufficient regulations to effectively regulate hosting operations of this kind underscores the intricate aspect of combating international cybercrime. The obstacles encountered in attaining global legal cooperation in addressing these difficulties highlight the pressing need for transnational coordination in order to efficiently tackle cybercrimes.

The importance of Rogue Services' activities in undermining cybersecurity and social safety is appropriately underscored by its engagement in facilitating the distribution of spam, spyware, malware, and ransomware. The multifaceted nature of cyber threats is shown by its possible ramifications, which include financial losses, data breaches, and interruptions to company operations. These repercussions serve to emphasise the seriousness of such threats across many domains. This component aptly demonstrates the concrete, practical consequences of cybercriminal operations in the real world.

The ethical analysis of Rogue Services' activities, as presented in the BCS Code of Conduct, reveals a clear deviation from the standards of honesty, professional competence, and professional obligation. This explication provides vital insights into the ethical implications of their behaviour. In addition, the user's perspective on the detrimental impact of their conduct on the reputation of the computer field is consistent with the British Computer Society's commitment to maintaining ethical standards within the industry and promoting the disclosure of unethical behaviours (British Computer Society, 2022).

Your discerning remark on the incongruity between Rogue Services' behaviour and their professed dedication to professional growth adds a significant dimension to the study. This remark highlights the significance of ethical deviations in eroding the fundamental principles of professionalism and the need of ongoing development.

Reference:

ACM (N.D). ACM Ethics. Available at: https://ethics.acm.org/code-of-ethics/using-the-code/case-malware-disruption/ [Accessed 18 August 2023].

British Computer Society (2022) BCS Code of Conduct. Available at: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/ [Accessed 17 August 2023].