Research Methods and Professional Practice March 2022

« Collaborative Learning Discussion 1

Victor Javier Martinez Hernandez

Initial post

76 days ago

1 reply

Last 69 days ago

Rogue systems infringed several codes of conduct when defending their “no matter what” policy, as the case tells, it seems that those in charge of the company were aware of the SPAM and malicious systems that were working on their network.

The ISP did not try to suspend those clients that were actively causing harm to third parties, following its policies, the solution was to disrupt their services using a ‘worm’ that attacked only the internal network of Rogue systems.

From a moral and ethical viewpoint, both actions had unethical conduct, as the data of third parties were destroyed, and even when arguing that it was for a greater good (Mitchel, 2018), there must have been more considerations for those that have no participation in the way Rogue systems were conducting their business and have their services disrupted.

Issue	BCS	ACM
Allowed malicious software defending a commercial policy	1a - have due regard for public health, privacy, security, and wellbeing of others and the environment.	1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing 1.2 Avoid harm

	2f - avoid injuring others, their property, reputation, or employment by false or malicious or negligent action or inaction. 2g - reject and will not make any offer of bribery or unethical inducement.	2.8 Access computing and communication resources only when authorized or when compelled by the public good. 3.1 Ensure that the public good is the central concern during all professional computing work.
Worm authors disrupting ISP service and destroying third-party data	1a - have due regard for public health, privacy, security, and wellbeing of others and the environment 1b - have due regard for the legitimate rights of Third Parties. 2f - avoid injuring others, their property, reputation, or employment by false or malicious or negligent action or inaction.	1.2 Avoid Harm 2.8 Access computing and communication resources only when authorized or when compelled by the public good.

References

ACM (2021) ACM Code of Ethics and Professional Conduct. Available from:

https://www.acm.org/code-of-ethics

[Accessed 11 March 2022].

bcs.org (2021) BCS, The Chartered Institute for IT code of conduct for BCS members. Available from: https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf

[Accessed 11 March 2022].

Mitchell, J. (2018) Ethics vs morality. Available from: https://www.bcs.org/articles-opinion-and-research/ethics-vs-morality/. [Accessed 13 March 2022]

Reply

1 reply

1 

Post by **Shoumik Chakraborty**
Peer Response

69 days ago

The post describes the destructive actions of both the Rouge Systems and the Government & Security Vendors.

It is important to note, "Despite repeated requests from major ISPs and international organizations" (Association for Computing Machinery, N.D.) Rouge had not stepped in to amend changes in their service, so the ISP providers had requested Rouge not to host malicious websites.

Legally "Rogue was based in a country whose laws did not adequately proscribe such hosting activities" (Association for Computing Machinery, N.D.) thus, Rouge Systems are not committing any crimes in the country of network hosting.

The major ISP providers and government officials could have fully or partially black-listed the IPs and DNS of the services hosted by Rouge System or could have identified and blocked the malicious websites and services. There are several examples of blocking by ISP for example, in certain regions government blocks VoIP (Turak, 2020).

The response team had other options to countermeasure threats from Rouge Systems but indulged in data destruction of criminals and innocent as the same.

References

Association for Computing Machinery. (N.D.) Case: Malware Disruption. Available from: https://ethics.acm.org/code-of-ethics/using-the-code/case-malware-disruption/ [Accessed 20 March 2022].

Turak, N. (2020) CNBC.UAE loosens some VoIP restrictions as residents in lockdown call for end to WhatsApp and Skype ban. *CNBC.* Available from: https://www.cnbc.com/2020/03/26/coronavirus-lockdown-uae-residents-call-for-end-to-whatsapp-skype-ban.html [Accessed 20 March 2022].

Reply

Maximum rating: -

Add your reply

Your subject

Type your post

Choose Files no files selected

Submit

Use advanced editor and additional options

Older discussion

Summary Post

Newer discussion

Initial Post