**Case: Malicious Inputs to Content Filters**

**Using the Code: Malicious Inputs to Content Filters**

The argument is controversial because the Rogue used a seemingly procedural justice to condone cyber crimes but the means of the just did not strictly conform to procedural justice. Rogue Services claims that its services have pledges such as 'no matter what' which means they do not intervene in the customer's activities. The truth is such a lack of supervision leads to the abuse of malware and spam use of their services. But in the end, Rogue was destroyed by some security vendors and government organizations, although they used an unofficial way. I would analyze this case from the perspective of four ethical frameworks which are Deontology, virtue Ethics, Utilitarianism, and Social Contract Theory, respectively.

Deontology: According to Immanuel Kant, Rogue's services violated some principles of the rules such as hosting malicious software and causing infections, which means the company should suspend the malicious clients's accounts and accept the ISP's requests. However, the government organizations that have taken offline Rogue's services may also violated some rules that they must obey the law to shut down the services but not simply use denial-of-service attacks to stop it. The inflexibility of Deontology makes the situation tricky and may cause some devious crime rampage.

Virtue Ethics: As for Ethics, what Rogue has done clearly violated almost every six core values in our society identified by the Josephson Institute of Ethics. The services they provided were not trustworthy to the public, and the company was not respected because they were not responsible nor caring for the public good. But justice is also hard to evaluate according to Ethics. The government organizations smashed the company not obeying any explicit rules but only the view of some government organizations. Other governments or organizations may have different ethical values.

Utilitarianism: According to Utilitarianism, the Rogue must shut down regardless of the means because the outcomes of the offline services cause more benefits than harm. Additionally, the offline of Rogue may cause some innocent customers of Rogue's service to face damage but it's less than the damage caused by ransomware rampage. Utilitarianism is an attractive approach that provides a clear and practical method to the problem, but the way that 'ends justify the means' logic may cause danger in the future. How could we know that the government may not give an order to attack Twitter, GitHub, or other web services that may offend some VIP's pride or interests?

Social Contract Theory: The Social Contract Theory may agree to punish Rogue by setting up a web services rule but not simply attacking it to offline the services. If the ISP and governments form a web services rule, Rogue must obey it or get punished. But the cunning company may find a country where the government does not join the rule and it is hard to persuade every corner of the world to obey one internet law. A social contract is hard to form in one country and it is even harder over the world. Especially on the internet, what could we do to the web server in another country? Simply banning it may cause another ethical problem. At least the Social Contract Theory may give us a chance to solve the ethical problem, and we should consider the trade-off between civic rights and cyber security.