Malware Report

**What are the risks and possible unintended consequences that could result from law enforcement’s plan?**

The risk and possible unintended consequence that could result from law enforcement’s plan is high. Reason being is that malware taxonomy can be very complicated, as methods to KILL command to shut down the malware is not guaranteed. Hence, without proper knowledge of the malware, this could be a big rest for the future development.

There many different computer architectures, operating systems, and network topologies Potentially, the law enforcement plan may not work on the difference of devices that they come across.

**Do you think that such a plan is a good or a bad idea given the risks you identified?**

First off, having a plan is a good start. Being aware of the malware and having an initial temporary plan, as it gives time to make a dynamic plan in the future. Being aware of which devices are affected should be noted, because there would be a potential of an attack in the future.

**What would your recommendation be?**

In my opinion, I would take note of which devices were affected plus the potential of other devices that could potentially communicate with as it was in the same network. There would be two scenarios reason being how significant this can affect the company or government official, as sometimes data could be potentially sensitive, or the cost and time is limited. First off, the first scenario I’d isolate those devices and replace them for example computers, routers, and data. Reason being there could have had rootkits installed or even worms embedded in the files in which it could potentially affect the new devices and potentially have an attack in the future. A second scenario were we create a different Information technology architecture system which doesn’t have contact with those devices noted, and closely observe the system for penitential malware still embedded. These methods are depended on cost, time and data sensitivity.