**Incident Report #:** IR-785

**Reported Date and Time:** November 16, 2015

**Technician:** Yifan Zhang

**Site Location:** VSCLvWorkstation

**Identification (Type and how detected):**

We regularly use AVG anti-virus software scan our workstation. And, we found there are many virus existing in a folder of our workstation’s C drive.

**Triage (Impact):**

Based on our investigation, these viruses don’t infect and spread from the network which means that they only negatively impact the infected hosts. However, these viruses might cause serious data compromise of the local computer.

**Containment (Steps taken):**

1. Back up all the critical data in this system
2. Find out the process that the viruses are running on
3. Kill these processes. If we cannot kill them, we need to reboot our computer into safe model and then try to stop those processes or use anti-virus software clean the infected files.
4. Delete all the entries related to virus in Windows Register
5. Restart the host.

**Investigation (Cause):**

The reason why this incident happens is that the host’s end user downloaded an infected zip file which bypasses our security settings. Then, he unzipped this file into his C drive. Later, he clicks one of the execution file in that unzipped folder and as a result the host is infected with virus.

**Recovery and Repair (Resolution):**

We use antivirus software to remove those infected files and we installed anti-virus software like AVG in every host in our company. The AVG can run at the background, when it detects dangerous, it will prompt user about virus detection.

**Lessons Learned (Debriefing and Feedback):**

From this case, we learn that every host should have its own anti-virus software installed instead of only using the enterprise level intrusion detect and prevention system. Education and trainings about security awareness should be scheduled periodically – maybe two month as an interval. Strengthen our information security inspection; especially disable those web requests from a dangerous IP address.