Write Up

The last weeks we’ve talked about malware dissection and offense, but this week we discussed malware defense. There are various ways to protect your network infrastructure from malware defense, but in my research, I found nothing is more effective than network segmentation and virtualization. By layering your defense, you make it difficult for malware to penetrate your network infrastructure and in the event they succeed, make it difficult in scanning and exporting valuable data.

As discussed in the lecture, there are static and behavioral methodologies in detecting potential device compromises. Some examples include:

* Network firewalls
* Install antivirus on hosts
* Access control policy
* Group policy for particular divisions of a business
* Host agents that report on suspicious files and behavior anomalies

Furthermore, there are tools simple enough to aid your efforts for malware defense. In the lecture, we discussed Yara and Cuckoo. Tools simple enough and open source that allow it to be used by large to small businesses and personal consumers. These applications allow you to create rules where you define certain information to find when scanning files and directories.

There are other open source projects that involve the monitoring of host machine behaviors. One example is the Open Source HIDS Security or OSSEC. Per the documentation on OSSEC GitHub’s page, OSSEC is actively monitoring all aspects of Unix system activity with file integrity monitoring. Log monitoring, rootcheck, and process monitoring. A commercial counterpart to this project is Carbon Black.

Furthermore, through virtualization, IT professionals can now deploy virtualized app and desktop solutions for applications considered high risk, specifically applications with access to the external internet (i.e. web browsers). By hosting applications on VDI’s, if a user visits a site with malware injection the malware only affects the virtual system and is denied access to the host or server hosting the virtual session. This makes it easy to quarantine and remove the infected virtualization and restore a recent backup.