Defense Against the Dark Arts

Week 1 writeup

CS373.400 Winter 2018 Shoshana Abrass abrasss@oregonstate.edu

This first week we covered basic definitions and language, and then simple forensics: using tools to track what malware is doing on a system.

There are many different types of computer malware, and to be honest I found the lecturer's off-the-cuff definitions weren't always helpful. In particular I wanted to understand the difference between a virus and worm - and it remains somewhat unclear :)

Virus: "the defining characteristic of viruses is that they are self-replicating computer programs which modify other software without user consent."[1] Viruses may or may not have destructive behaviors.
Worm: "A standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer."[2]

In sum, it seems that worms are viruses that replicate using network access, whereas viruses are spread on a local computer, eg, by infecting local files which may then be shared on USB drives or via email. Now I know.

The lectures mentioned polymorphic malware several times because it can't be tracked with a hash signature. I didn't know that hashes were the primary identification system for endpoint AV software - but security is evolving very quickly so that may no longer be true. Even in the last few years, since the lectures were recorded, there are new tools that use large datasets to look for 'bad behavior' instead of a particular file signature[3]. The lectures do mention crowdsourcing signatures, eg with VirusTotal.

One thing that the polymorphic discussion made clear is that it's actually extremely difficult to find malware on host computers without using a lot of local resources. Even innovations, such as imphash detections, are easy to circumvent: in order to match the imphash, DLLs and other imports need to be loaded in exactly the same order.[4]

---

[1] Wikipedia entry for computer virus
[2] Wikipedia entry for computer worm
[3] I'm thinking of CrowdStrike, but I can't find a good reference
[4] https://www.fireeye.com/blog/threat-research/2014/01/tracking-malware-import-hashing.html

The other piece of information that was relatively new to me is the availability and usefulness of malware "kits" that can simply be purchased. This more than anything seems to be responsible for the dramatic increase in the sheer number of bad actors over the last decade. I'm hoping that future lectures go into this subject in depth.