Deniz Aytemiz
denizaytemiz@vt.edu

ECE 5480: Assignment 3

1. Computer viruses and worms are similar in terms of propagation. They both use self replication in order to propagate. Both of their rates of propagation over time can be modeled with epidemic model. However, while viruses need human interaction to spread in most cases ,such as opening of an email attachment, worms do not necessarily need that to propagate. They differ since viruses infect other programs and files to copy itself yet worms do not affect the other programs. On the other hand, the Trojan horse does not self-replicate. It can be controlled remotely like worms and unlike viruses. They require human assistance in order to launch into the system. Their rates of propagation are less than viruses and worms.
2. The online advertising space is complex which involves multiple redirections between different servers when a user clicks on an ad. The attack 'malvertising' occurs when an attacker injects malicious code into legitimate advertising networks. When a user views the webpage with malvertising content, by leveraging browser vulnerabilities the malware can be installed on the users computer. Or the malicious advertisement may cause the web page to redirect to a malicious website.
3. If a malware instance has different signatures, this would make it easier for the code to be undetected. Since malware detection systems have a list of detected signatures of malwares using multiple different signatures for the same vulnerability attacking malwares make it less likely to be detected by anti malware systems.
4. In that case, the diversity of the internet browser dramatically reduces. Which is risky for the Internet since there would be only one browser target for cyber attackers to exploit the vulnerabilities of and it would most probably be exploited. However when there are multiple browsers, if one is exploited the other can be used for access. Or at least it divides the focus of cyber attackers since all of them would most probably have different vulnerabilities due to different inner structures.
5. IoT devices have become the weakest link in terms of security point of view. Their naive security configurations, ubiquitous use and their connection to other devices with the internet makes them a starting point for bad actors to attack the entire IoT system. Mirai botnet is an example of IoT attacking malware causing Denial of Service. Mirai starts the attack by randomly searching for public IP addresses (with the exception of government related ones) through a TCP port. Then by brute force it discovers the credentials of a weakly configured IoT device. After obtaining the credentials and gaining access to the shell, the attacked device's characteristics and information about other devices in the network are forwarded to the report server from a different port. The communication between the infrastructures of Mikia's system is conducted with anonymous network Tor. Meanwhile the C&C continuously checks in with the report server for current status and other vulnerable devices to devices to attack. After selecting the new victim, botmastre issues infect command in the loader. Then the loader logs in to target devices and instructs the hardware to download and execute the binary version of the malware. When malware is executed it initially shuts down other the intrusion points to avoid other malware gaining access to the device. Device resolves a domain name in the executable and now is ready to get attack commands from C&C server. The C&C server instructs all bot devices to attack the main server by giving the information of IP addresses of the devices, target server and the duration of the attack. Then the bot devices use GRE,TCP or HTTP flooding attacks for the target server. Unlike similar malware Miria leaves behind a footprint of stages of infection that can be deduced from analyzing the Mirai's loader components' packet load and time graphic. With the source code of Mirai becoming public, a dramatic rise in the malware variants was observed. Some use the same basics with addition of encrypted C&C server communication channel and customed iptables

rules. Or instead of centralized architecture, distributed architecture such as BitTorrent DHT protocol is utilized with addition of encryption of the communication between bot devices. The security issues for vulnerable IoT devices must be taken care of in no time. Contrary to the belief, they are powerful enough to cause DDos attacks. In order to make them more secure, they should have on-off cycles and other protective measures like computers do. They should have more of a user interface to detect any malicious intent.