Kai Davids Schell

2: One virus that propagated incredibly virulently was the ILOVEYOU worm. The worm appeared in the form of an email with the subject line “I LOVE YOU” or something similar. In the email was a file with a .vbs extention that was hidden by default, causing users to believe that they were opening an innocent text file. The script contained then deleted data on the victim’s computer, and sent itself to everyone in the victim’s Microsoft Outlook address book. It is unknown exactly how many computers were infected, but it was over 45 million computers, an estimated 10% of all internet connected computers. The worm was eventually traced back to two Filipino programmers Reonel Ramones and Onel de Guzman.

3: The 4 levels of threat can be divided down to “No threat, Weak threat, Strong threat, Extreme threat’ and each breaks down further, based on the damage they might do.

No threat is self-explanatory.

Weak threat incudes agents with little motivation to exploit an authenitfication system and very little damage done.

Strong threat includes someone with the motivation and skills to overcome authentification, but a desire not to do visible or extreme damage, as well as someone willing to cause visible, but limited damage.

Extreme threat is any agent with the means and motivation to attack a system and cause significant damage to it, potentially resulting in injury or death.

4: The five basic attacks are

1. Copy/borrow the authentification token
2. Sniff it (intercept and copy it while the login is taking place)
3. Trial and error guessing
4. Denial of Service (Damaging the system, or unsuccessfully trying to log in enough that access is denied to the owner)
5. Retreive from offline (finding the authentication information or database and copying it)

5: Password hashing works by taking the user’s password and running it through a “hash function” that spits out some kind of gibberish that can’t be turned back into the user’s password, but it spits out the same output given the same input, to authenticate then, the server/OS/whatever stores only the hash, and when the user enters their password it runs it through the hashing function and compares it to the stored hash.

6:

1. Triple Data Encryption Standard:

Sources Cited

"What Is ILOVEYOU Virus?" *SearchSecurity*. TechTarget, Feb. 2006. Web. 06 Mar. 2016.