Agenda

- Review: The Seven Domains of a Typical IT Infrastructure
- Malicious Software
- Case Study: The Mirai Worm, Who is the Author?
Malicious Software

Malware for short

- Viruses
- Worms
- Trojan Horses
- Rootkits
- Spyware
Malicious Software

"What's the difference between viruses, trojans, worms, etc?
It doesn't matter. It's all crap no one wants on their computer.
Stop teaching users worthless information they'll never use."

- Taylor Swift

image source: @SwiftOnSecurity on twitter
Malware

- Infecting programs: actively attempt to copy themselves to other computers; main purpose is to carry out an attacker’s instructions on new targets. Viruses, worms fall into this category.

- Hiding programs: hide in the computer, carrying out the attacker’s instructions while avoiding detection. Trojan horses, rootkits, spyware belong to this category.
**Virus**: a software program that attaches itself to or copies itself into another program on a computer. The purpose of the virus is to trick the computer into following instructions not intended by the original program developer: Users copy infected files from another computer on a network, from a flash drive, or from an online service. A computer virus acts in a similar fashion to a biological virus. It "infects" a host program and may cause that host program to replicate itself to other computers.
**Worms**: a self-contained program that replicates and sends copies of itself to other computers, generally across a network, without any user input or action. The worm’s purpose may be simply to reduce network availability by using up bandwidth, or it may take other nefarious actions. The main difference between a virus and a worm is that a worm does not need a host program to infect. The worm is a standalone program.
**Trojan Horses**

*Trojan Horse*: also called a trojan, is malware that masquerades as a useful program. Trojan horse programs use their outward appearance to trick users into running them. They look like programs that perform useful tasks, but actually, they hide malicious code. Once the program is running, the attack instructions execute with the user’s permission and authority.
Rootkits: a rootkit modifies or replaces one or more existing programs to hide trace of attacks. Example: replacing ls, ps, cat with a malicious version of ls, ps, cat.
Spyware: a type of malware that specifically threatens the confidentiality of information. It gathers information about a user through an Internet connection, without his or her knowledge. Once installed, spyware monitors user activity on the Internet. Spyware can also gather information such as email addresses and even passwords and credit card numbers.
Case Study: the Mirai Worm

Mirai co-author Anna-Senpai leaked the source code for Mirai on Sept. 30, 2016.

image source: krebsonsecurity
The Mirai Worm

- A malware that turns computer systems running Linux into remotely controlled "bots", that can be used as part of a botnet in large-scale network attacks.
- It primarily targets online consumer and devices such as remote cameras and home routers.
- The Mirai botnet has been used in some of the largest and most disruptive distributed denial of service (DDoS) attacks, including an attack on 20 September 2016 on computer security journalist Brian Krebs’s web site, an attack on French web host OVH and the October 2016 Dyn cyberattack.
- Named after the 2011 TV anime Mirai Nikki.
FBI questions Rutgers student about massive cyber attack

The FBI has interviewed a Rutgers University student in connection with a series of cyber attacks last year after a computer security blogger said some of the coding used appeared to reach back to the student. His family said he is innocent and being falsely accused. (Photo by Shutterstock)

By Adam Clark and Mark Mueller | NJ Advance Media for NJ.com
on January 20, 2017 at 4:47 PM, updated January 20, 2017 at 9:52 PM
Rutgers student blamed for ‘worst internet attack in history’

By Dan Alexander  January 25, 2017 10:07 AM
Paras Jha, 20-years-old, the owner of ProTraf Solutions, a Minecraft-focused DDoS protection provider - Minecraft is a wildly popular computer game sold by Microsoft that can be played from any device and on any Internet connection.

Paras Jha is also a student at Rutgers University. This is especially notable because Rutgers has been dealing with a series of DDoS attacks on its network since the fall semester of 2015 more than a half dozen incidents in all. With each DDoS, the attacker would taunt the university in online posts and media interviews, encouraging the school to spend the money to purchase some kind of DDoS mitigation service.

So far, Jha has not been charged with any crimes and has not been named a suspect by authorities.
A large portion of the material is adapted from:

- Fundamentals of Information Systems Security - David Kim, Michael G. Solomon
- Who is Anna-Senpai, the Mirai Worm Author? https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/#more-37412
- Mirai (malware) - wikipedia