# Recommendation to counter dos attack

Engineering, Computer Security

Recommend in an executive summary measures to counter this type of DoS Attack.

The university network was a victim of a DDoS attack. Whereby a cyber criminal first acquired administrator access. We suspect that the attacker gained access to the network from an internal computer, most likely from a student PC in one of the labs. The attacker likely used keylogger software to discover administrator credentials.

Once the attacker had the administrator access the systems he/she was able to create BOTs and push to many student PCs located in various labs. The attacker then initiate a control attack by activating the BOT's in order to form a BotNet (a. k. a. Zombie Network) with the goal of intentionally causing online services to become unusable to students (ICECC, 2009). It is important to note that a single BOT alone could not have cause the registration server unavailable. It was the combined effect of using many BOTs at once that produced the attacker's desired effect of overflowing the resources of the registration web server and rendering it unusable.

Recommendation to Counter this type of DoS attack

To prevent or limit the impact of keyloggers: Deploy a firewall to block known keylogger software. Educate facility not to open email from unknown users and not to click on links in emails from unknown users. Create a Policy whereby users cannot install new software to a machine without opening a ticket with the helpdesk or requesting administrator access (ICECC, 2009). The student computers should be preloaded with all required applications.

Deploy a file monitoring program, such as Tripwire to detect and notify if any changes have occurred to files (ICECC, 2009). Passwords should always be encrypted and never traverse the network in the clear. Harden Windows by making sure that the operating system are keep current with latest patches (ICECC, 2009). Keep anti-virus, anti-spyware programs up-to-date.

Install firewall packages on all computers.

Deploy an intrusion-detection (IDS) and intrusion-prevention systems (IPS). Segmenting off network with the use of routers or firewalls is another method (Schifreen, 2006). However, the routers or firewalls will have to be configured to detect and block suspected BOT traffic (please see network diagram for item with Blue Dotted Squares).

Conclusion

It is important to note that there is no method that will secure a network totally from attack. However, we can prevent some of the most common attack vectors. Therefore security personnel must remain vigilant and seek to prevent the new level of attack (Schifreen, 2006).