Port Stealing

Port stealing is a man in the middle attack where a local area network switch makes attempts to intercept packets that are meant to go to another host by stealing from the intended port on that switch. This attack is meant to be used in the local area network only. The attacker uses the victim's stolen MAC address to force the switch to change its forwarding table, causing the packets sent to the victim's computer to be sent to the port the attacker is connected to. (Ettercap) From this point the attacker can read the information in the packets, cause a delay, or drop the packets from ever getting to the victim. Port stealing makes use of the switches connection between the binding of MAC addresses and the physical ports themselves.

A port stealing attack scenario could be executed during an online gaming competition. The attacker can delay the packets going through the switch from a competitor's system to cause lag/slowdown. The delay could be slight as to not cause suspicion but still allow the attacker to gain a competitive edge. In key moments during the game the attacker may increase the delay or even drop packets. This interference does not block traffic completely, but rather simply drops packets for short spurts rather than all together completely. If all competitors are connected on the same switch the attacker could even use port stealing to intercept packets from multiple systems at once giving them an even larger competitive advantage, which in itself is malicious towards an attackers competitors. This attack, however, would only work in this scenario as mentioned, where all players are connected through the same network, allowing the attacker to use this to their advantage.

Citations:

Baxley, Thomas, Jinsheng Xu, Huiming Yu, Xiaohong Yuan, Jinghua Zhang, and Joseph Brickhouse. "LAN Attacker: A Visual Education Too." InfoSecCD '06 Proceedings of the 3rd Annual Conference on Information Security Curriculum Development (2006): 118-23. ACM Digital Library. Web. 09 Nov. 2016.

Alzubaidi, Waleed Kh. "A New Verification Method to Prevent Security Threads of Unsolicited Message in IP Over Ethernet Networks." *International Journal of Computer Networks & Communications* 4.6 (2012): 21-31. Web.

Ornaghi, Alberto, Marco Valleri, Emilio Escoobar, Eric Milam, and Gianfranco Costamagna. "Read Me." GitHub. Ettercap., 31 Oct. 2016. Web. 10 Nov. 2016.