**MALWARE OPENING PORTS**

1. **Remote Access Trojan (RATs)** are malicious programs that run invisibly on host PCs and permit an intruder remote access and control. Intruders ultimately launch the server program on a victim's machine. (Intruders can use a program called a *binder* to combine RATs with legitimate executables so that the RATs execute in the background while the legitimate applications run, leaving victims unaware of the scurrilous activities.) In many cases, intruders can customize the server program: set IP port numbers; define when the program starts, what it's called, how it hides, and whether it uses encryption; customize logon passwords; and determine when and how the program communicates. After defining the server executable's behavior, the intruder generates the program, then tricks the host machine's owner into running it [1].

*Note:* These programs may be able to access *File System* or *memory* on the victim’s computer

**REFERENCES**

1. <https://technet.microsoft.com/en-us/library/dd632947.aspx>