How the Worm Simulation was Designed

The provided python script, worm_simulation.py, models Code Red and Code Red II worm propagation. The script starts runs through both worms 3 times each. Within each run it intializes the vulnerable and infected IPs, simulates the worm, and gathers info on the run time. The vulnerable IP addresses are grouped into clusters of 10 consecutive addresses, spaced every 1,000 IP addresses. The worm begins propagation from an initial infection at IP address 4009.

Each infected computer scans two (m = 2) IP addresses per discrete time tick. Newly infected hosts begin scanning after a delay of 30 ticks. Two scanning methods were simulated:

- Code Red, random-scanning method: Each IP scan randomly selects an IP address between 1 and 100,000.
- Code Red II, local-preference scanning method: With a probability of 0.5, the scan targets IP addresses within ±10 of the infected computer's IP; otherwise, it scans randomly across the entire IP address range.

The script outputs multiple .csv files containing data on each run.

Random-Scanning Simulation Results

Figure 1 shows the infection rate over time for three simulation runs using random-scanning

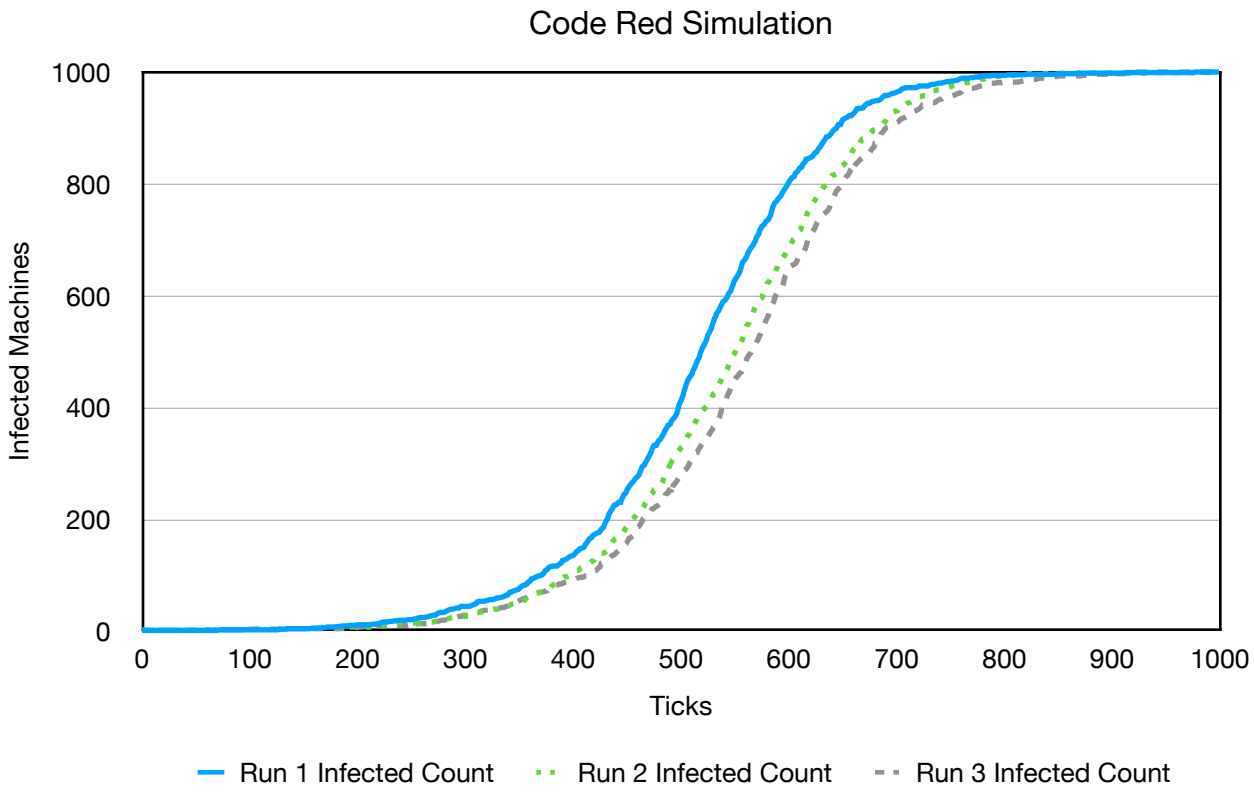

Table 1: Time for the worm to infect all vulnerable hosts in each run:

Code Red Simulation Stats

Simulation	Elapsed Time	Ticks
code_red_1	0.831	976
code_red_2	0.860	1000
code_red_3	0.900	919

Figure 2 illustrates the infection rate over time for three simulation runs using local-preference scanning

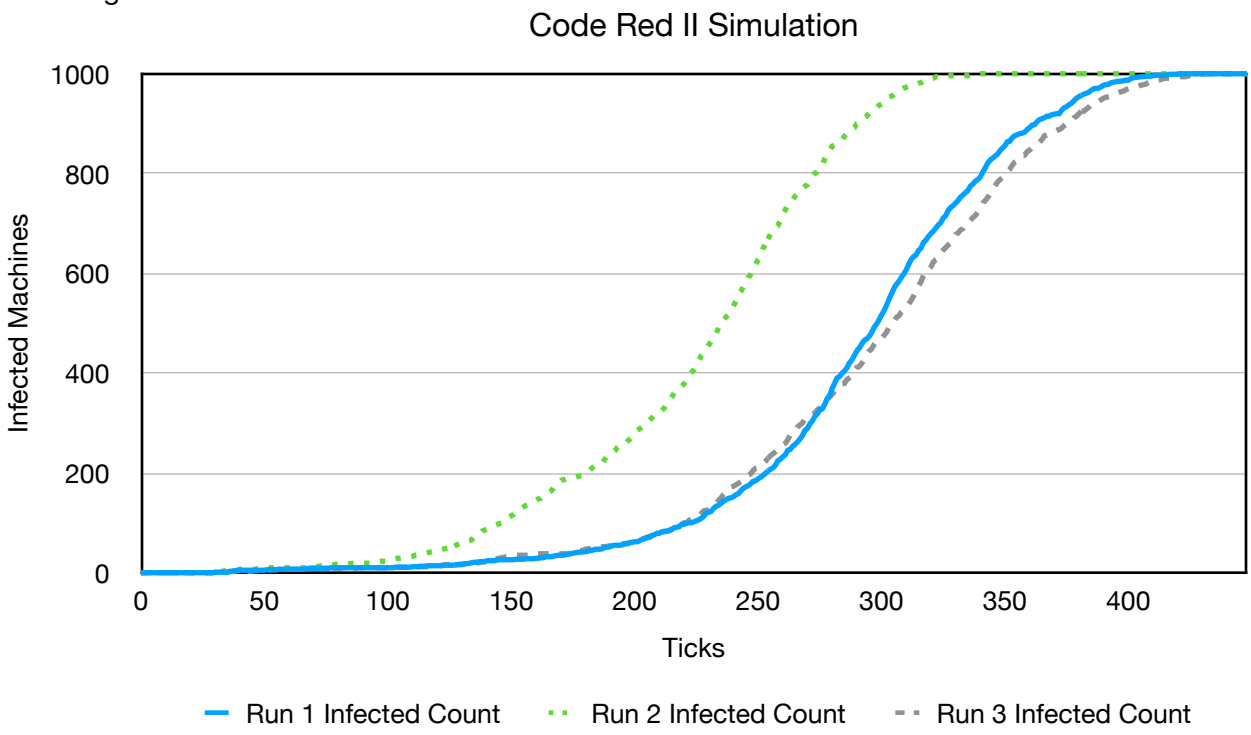

Table 2: Time for the worm to infect all vulnerable hosts in each run:

Code Red II Simulation Stats

Simulation	Elapsed Time	Ticks
code_red_II_1	0.251	421
code_red_II_2	0.226	340
code_red_II_3	0.275	431

How to run

To execute the simulation:

```
python worm_simulation.py
```