1. Code Red formulates the exploit string and sends it to the victim's Internet Information Server.

2. Since the victim's operating system is ESP-enabled the network stack has a sensor specifically designed to detect Code Red's exploit code.

3. Also, the victim was lucky enough to have a version of Internet Information server that has a more generic sensor to detect general buffer overflows. While this sensor is not specific to Code Red, it does provide the system administrator with a warning that an attack may be occurring.

4. The ESP framework provides the capability for sensor data to be transmitted in a secure and authenticated way.

5. Here we see that one of the places the sensor data can go is into a standard log file.

6. Another option is for it to be collected with other intrusion detection data into some sort of data correlation system.

7. Finally, if the data is deemed to represent a critical alert, it can be sent straight to a system administrator.

How ESP can detect Code Red