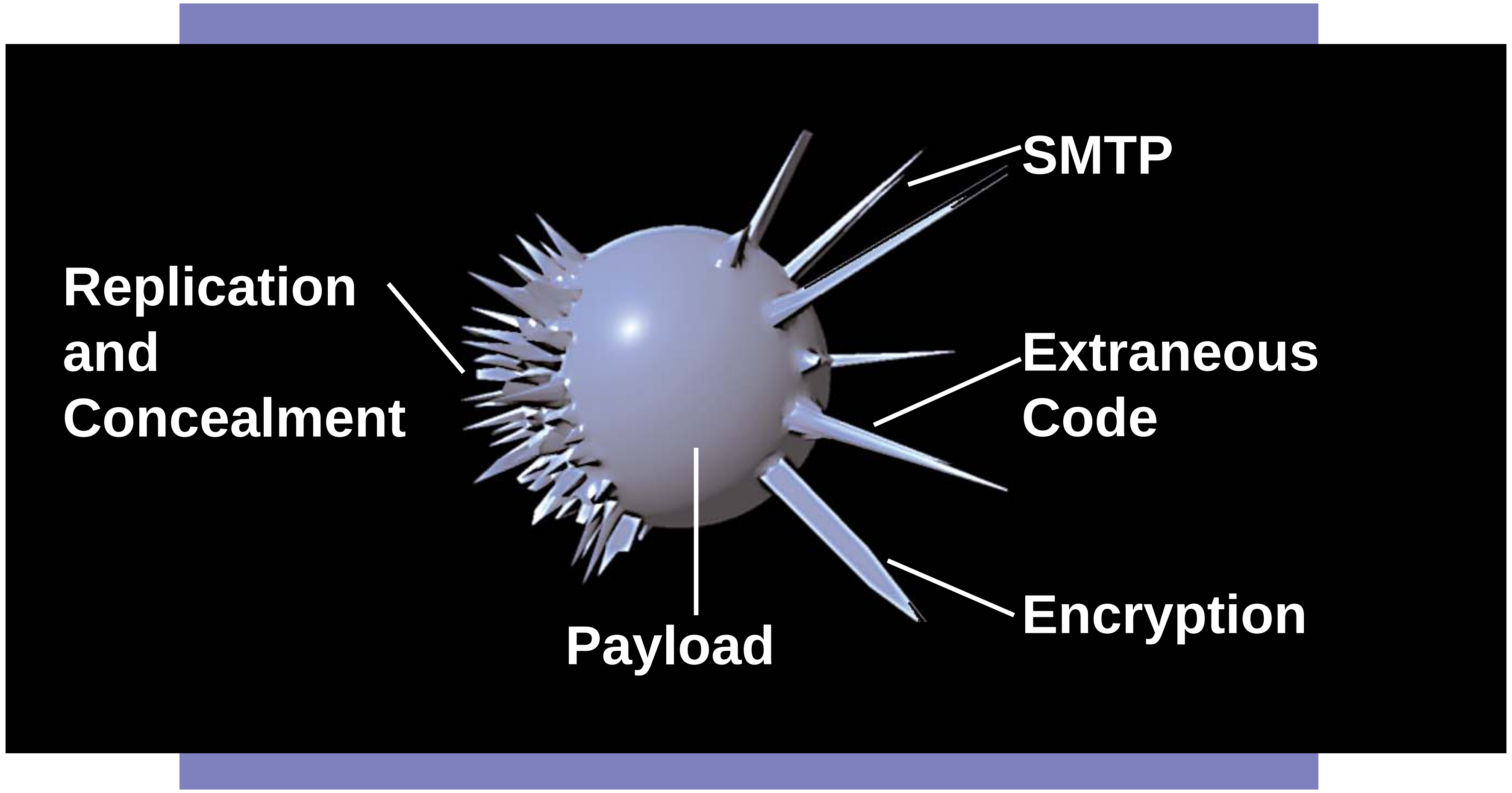
The Anatomy of a Virus



How it's contracted

- Through e-mail attachments and P2P file-sharing networks
- By opening an HTML e-mail
- Physically transferred from an infected home machine by CD or disk
- From infected commercial software, shareware, freeware, or data disks
- From a user visiting malicious Web sites either intentionally or by misdirection

How it spreads

- Exploits software flaws
- Uses bugs in common protocols such as SSL
- Exploits weaknesses in TCP/IP
- Understands human behavior
- Actively scans systems connected to the Net, looking for and exploiting known vulnerabilities

What a virus is

A virus is a program that automates an attack on a PC or network. It typically has malicious intent, ranging from disrupting access to computing power and stealing data to using your computer to attack other computers.

TechRepublic®
Real World. Real Time. Real IT.

Virus components

- Replication and concealment
- Payload such as a trap door or code designed to cause damage to the infected system
- Accessory code such as e-mail and encryption engines needed to run the payload, and extraneous code only intended to make the file larger and more difficult to analyze

Immediate remedy

For worms that keep shutting down the system too quickly for you to repair it, Microsoft recommends that you first try running shutdown -a from the command prompt. This is much faster than the five steps below and will also abort the shutdown process, but it might work only on XP systems.

Here are the first five steps toward detection and removal of the specific malware:

1. Disconnect from the Internet.
2. Reboot.
3. Click on Start | Run and enter *cmd* to open the command line interface.
4. At the DOS prompt, type *shutdown -i <ENTER>* and enter the name of your computer.
5. Modify the warning-message delay setting from the standard 20 seconds to a large number such as 9999.