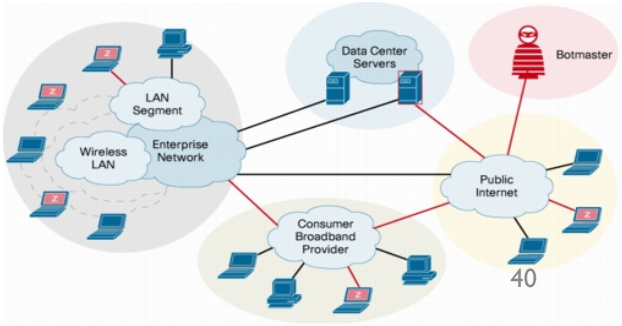
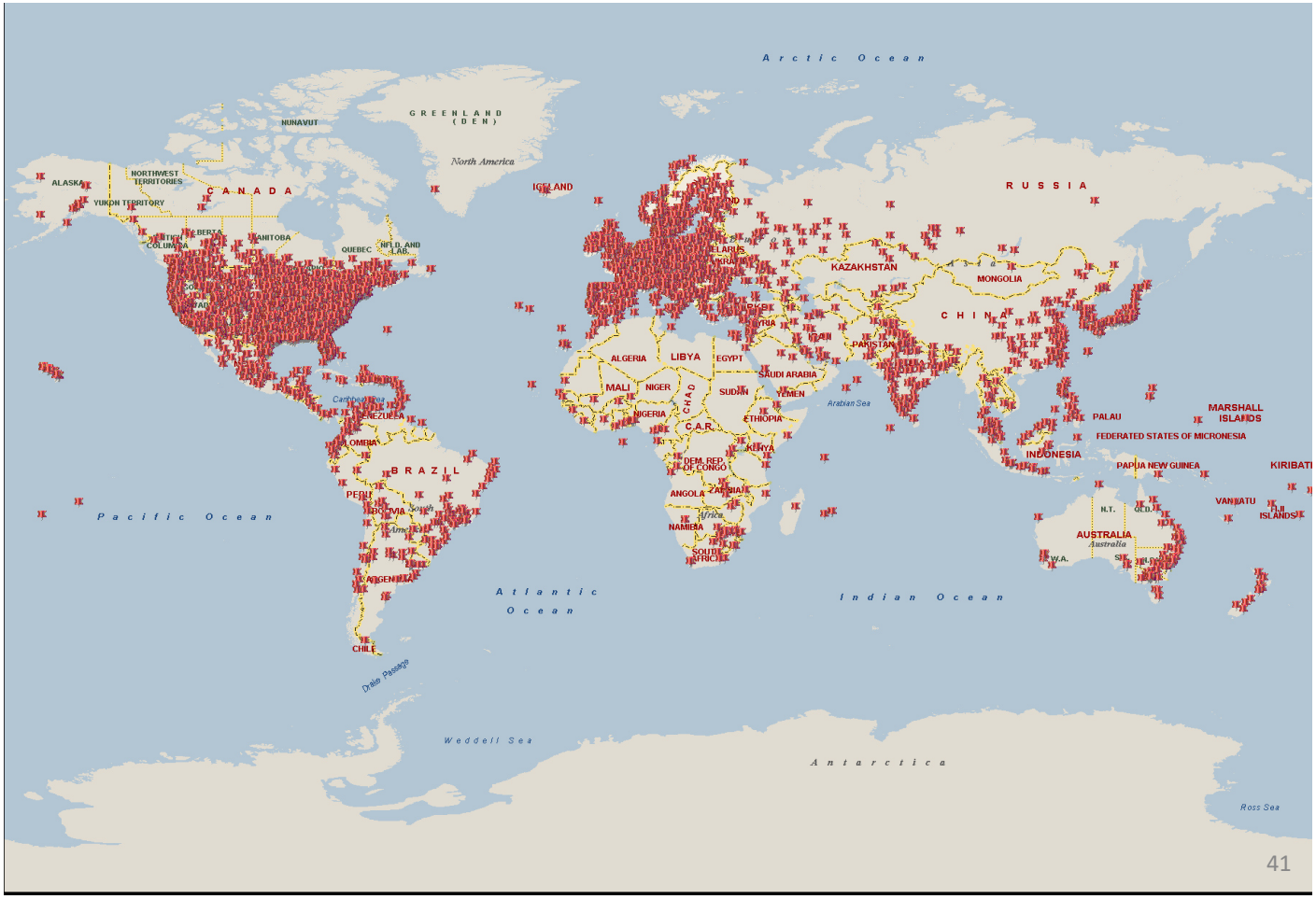
Botnets

- A large group of computers controlled from one or more remote locations by hackers, without the knowledge or consent of their owners
- Distribute spam and malicious code
- Cutwail, a large botnet, controlled approximately one million active bots at one time.
- In 2008, about 90 percent of spam was distributed by botnets, including the notorious Storm, Srizbi, and Cutwail botnets
- Quite expensive to deal with them



Computers infected by the Waledac botnet in a 18-day period



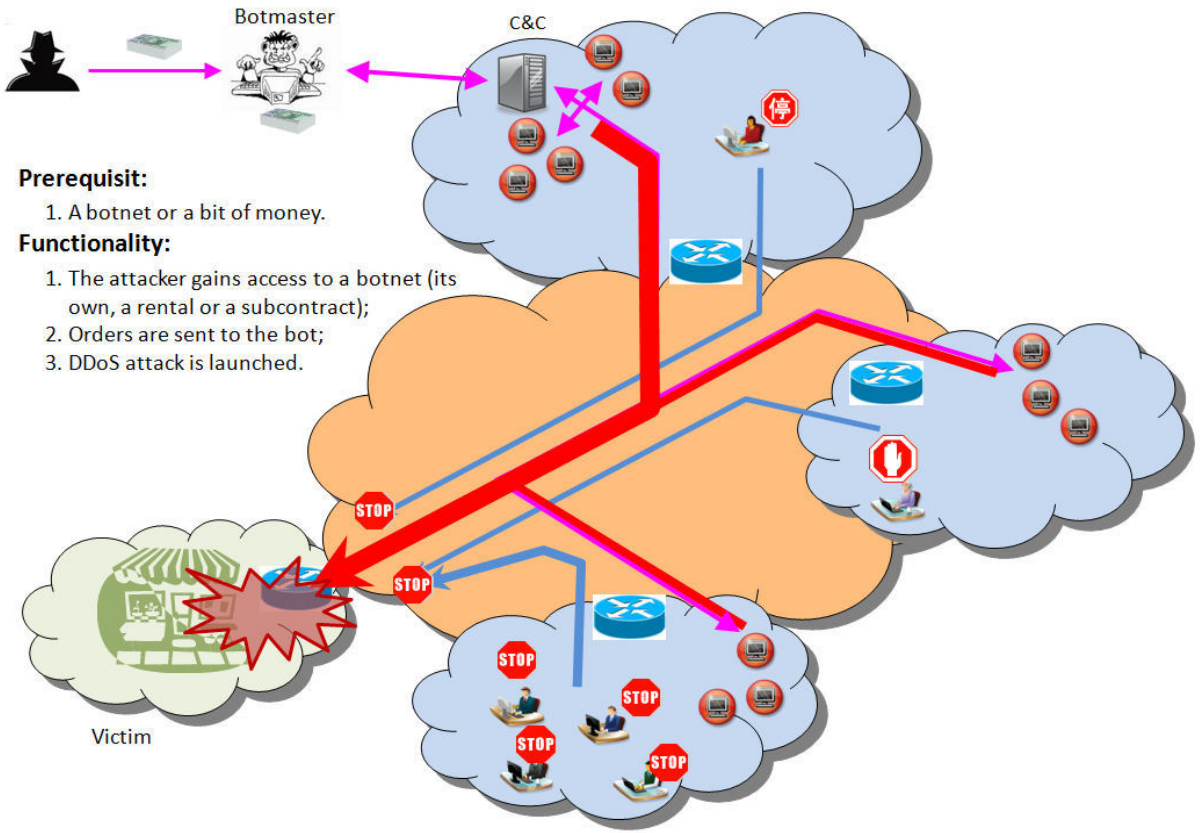
7. Denial-of-Service (DoS) Attacks

- Malicious hacker takes over computers on the Internet and causes them to flood a target site with demands for data and other small tasks
  - The computers that are taken over are called **zombies**
- Does not involve a break-in at the target computer
  - Target machine is busy responding to a stream of automated requests
  - Legitimate users cannot get in
- Spoofing generates a false return address on packets

Denial-of-Service (DoS) Attacks Countermeasures

- **Ingress filtering** - When Internet service providers (ISPs) prevent incoming packets with false IP addresses from being passed on
- **Egress filtering** - Ensuring spoofed packets don't leave a network

DDoS Attack: How it Works?



DDOS Attack: Solutions (I)

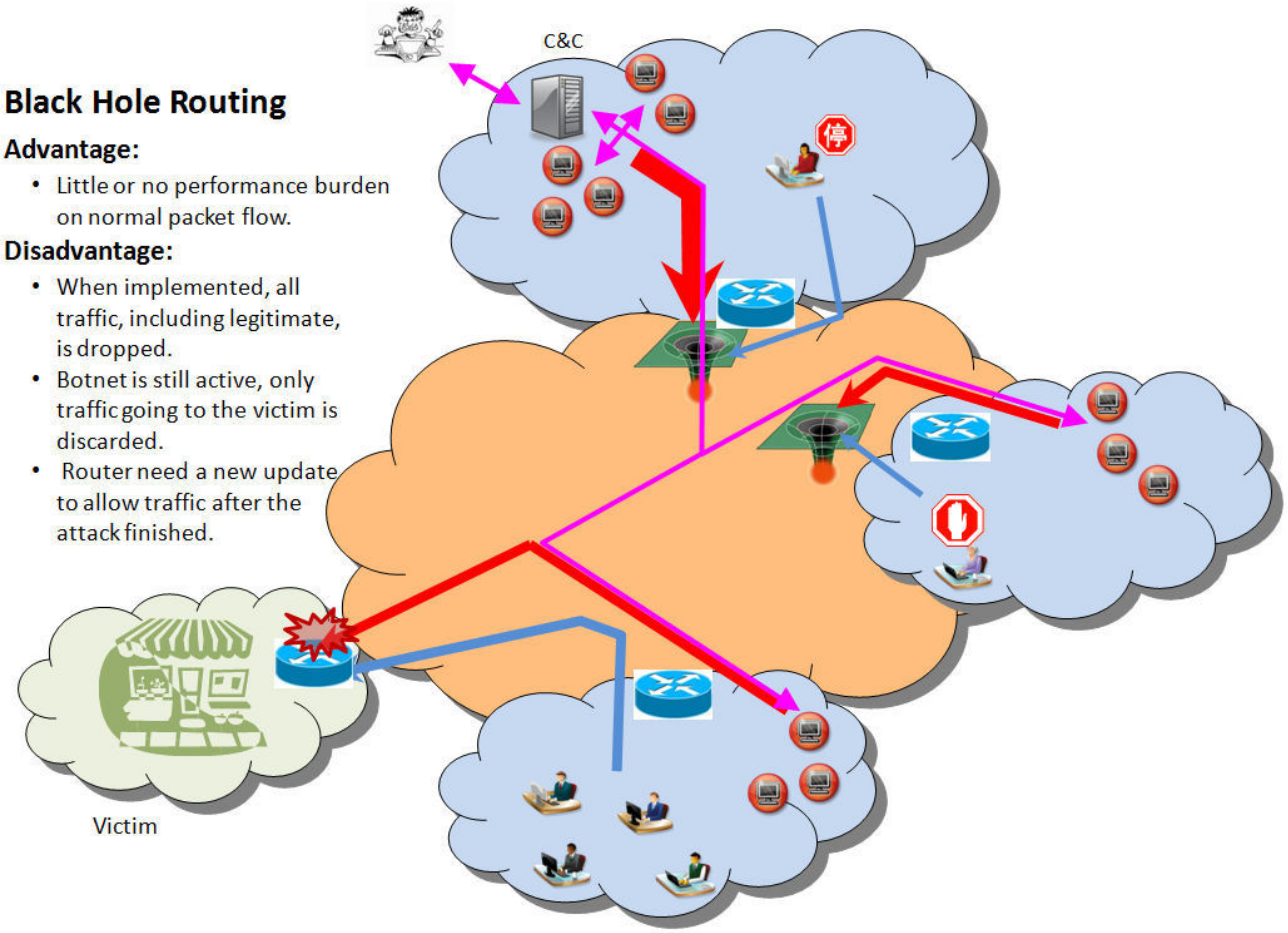
Black Hole Routing

Advantage:

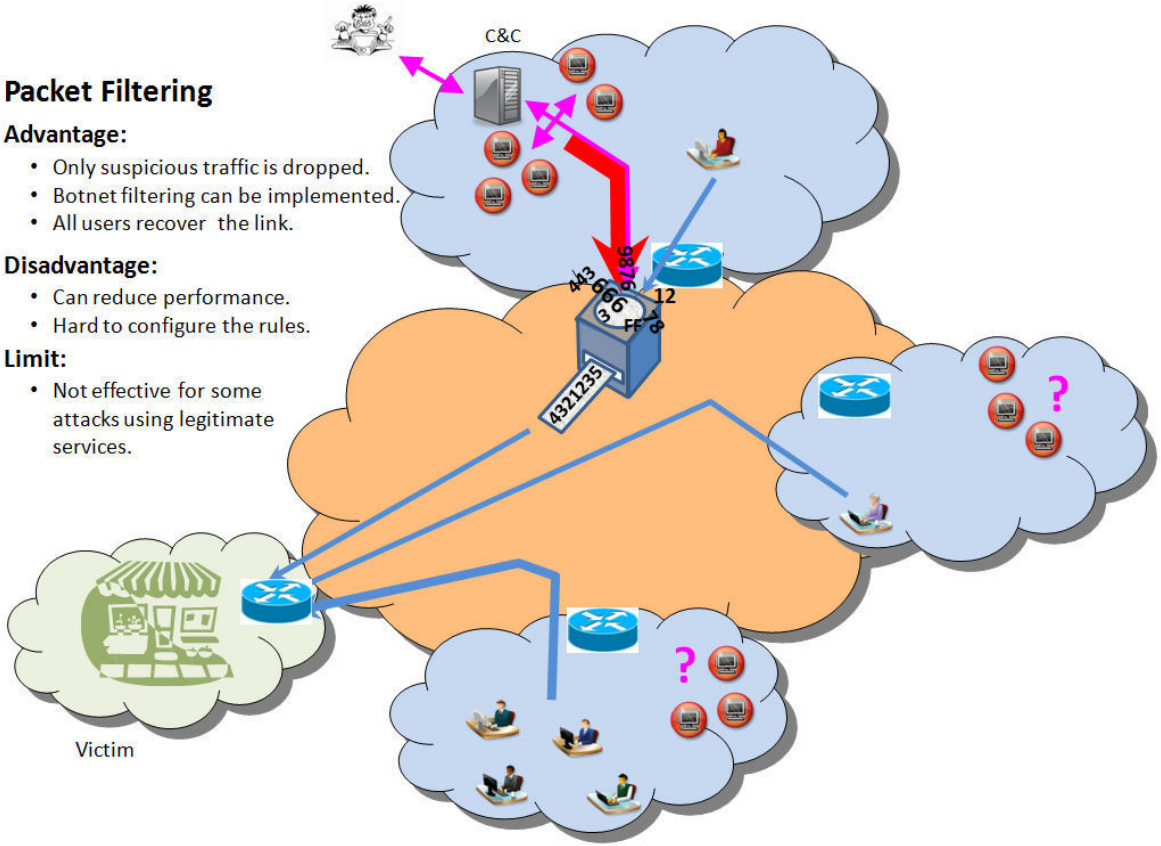
- Little or no performance burden on normal packet flow.

Disadvantage:

- When implemented, all traffic, including legitimate, is dropped.
- Botnet is still active, only traffic going to the victim is discarded.
- Router need a new update to allow traffic after the attack finished.



DDOS Attack: Solutions (2)



Denial-of-Service (DoS) Attack: Case Study

- The Republic of Estonia (population 1.4 million) in the Baltic region of northern Europe.
- Gained its independence in 1991.
- During April and May of 2007, a global botnet of compromised home computers was used to launch hundreds of coordinated DDoS attacks, which disrupted the Web sites of numerous **Estonian government agencies, financial institutions, and media outlets**.
- Pro-Russian activists led the attacks in retaliation for the Estonian government's decision to move a Soviet World War II memorial

8. Rootkits

- A set of programs that enables its user to **gain administrator level access** to a computer without the end user's consent or knowledge
  - **Dropper:** gets the rootkit installation started, launches the loader program and delete itself.
  - **Loader:** loads the rootkit into memory.
  - **Rootkit**
- **Symptoms** of rootkit infections
  - The computer locks up or fails to respond to input from the keyboard or mouse.
  - The screen saver changes without any action on the part of the user.
  - The taskbar disappears.
  - Network activities function extremely slowly.

9. Advanced Persistent Threat (APT)

- A network attack in which an intruder gains access to a network and stays there—**undetected**—with the intention of stealing data over a long period of time (weeks or even months)

- APT attacks target organizations with high-value information, such as banks and financial institutions, government agencies, and insurance companies with the goal of stealing data

APT five Phases

1. **Reconnaissance**—The intruder begins by conducting reconnaissance on the network to gain useful information about the target (security software installed, computing resources connected to the network, number of users).
2. **Incursion**—Launch incursions to gain access to the network at a low level to avoid setting off any alarms or suspicion, e.g., Spear phishing. The attacker establishes a back door, or a means of accessing a computer program that bypasses security mechanisms.
3. **Discovery**—Begin a discovery process to gather valid user credentials (especially administrative ones) and move laterally across the network, installing more back doors. These back doors enable the attacker to install bogus utilities for distributing malware that remains hidden in plain sight.
4. **Capture**—The attacker is now ready to access unprotected or compromised systems and capture information over a long period of time.
5. **Export**—Captured data are then exported back to the attacker's home base

Case Study: Carbank

- The hacker group Carbanak is thought to have stolen over **$1 billion** from banks in China, Russia, the Ukraine, and the United States.
- Use of an APT that initially hooks its victims using spear phishing emails
- Performed a reconnaissance phase to gather data about system administrators and then uses this information to navigate through various bank systems, including ATMs, financial accounts, and money processing services.
- Once access to these systems is gained, the hackers steal money by transferring funds to accounts in China and the United States.
- Even programmed ATMs to dispense money at specific time and location

10. Phishing

Act of using e-mail fraudulently to try to get the recipient to reveal personal data.

Spear-phishing is a variation of phishing in which the phisher sends fraudulent e-mails to a certain organization's employees.

11. Smishing and Vishing

Smishing is another variation of phishing that involves the use of texting. In a smishing scam, people receive a legitimate-looking text message telling them to call a specific phone number or log on to a website.

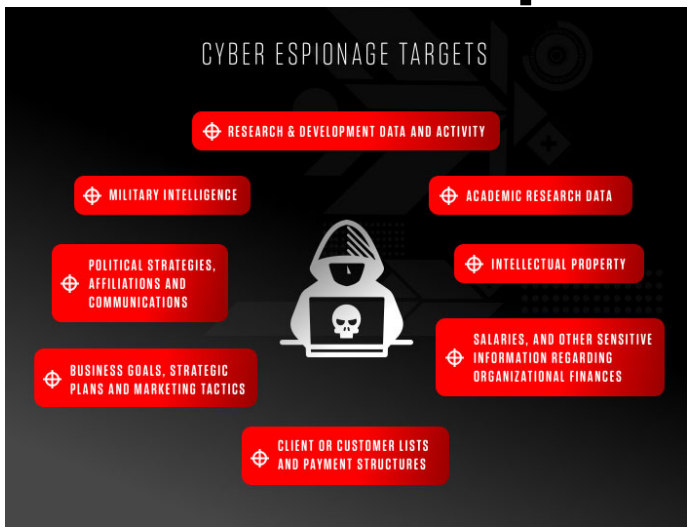
I I. Smishing and Vishing

Vishing is similar to smishing except that the victims receive a voice-mail message telling them to call a phone number or access a website.

12. Cyberespionage

Cyberespionage involves the deployment of malware that secretly steals data in the computer systems of organizations, such as government agencies, military contractors, political organizations, and manufacturing firms.

The type of data most frequently targeted includes data that can provide an **unfair competitive advantage to the perpetrator.**



High Value Data:

- Sales, marketing, and new product development plans, schedules, and budgets
- Details about product designs and innovative processes
- Employee personal information
- Customer and client data
- Sensitive information about partners and partner agreements

13. Cyberterrorism

Cyberterrorism is the intimidation of government or civilian population by using information technology to disable critical national infrastructure (for example, energy, transportation, financial, law enforcement, and emergency response) to achieve political, religious, or ideological goals.

It is an increasing concern for countries and organizations around the globe.