openHPI Course: Cyberthreats by Malware

Most Common Attacks

Prof. Dr. Christoph Meinel
Hasso Plattner Institute
University of Potsdam, Germany

Most Common Attacks on the Internet: **DoS and DDoS Attacks** (1/2)

Denial-**o**f-**S**ervice

- Attack aimed to disrupt the availability of a service on the Internet

Distributed **D**enial-**o**f-**S**ervice

- Denial of service attack carried out from many different stations in the Internet, e.g., executed via botnet

Most Common Attacks on the Internet: **DoS and DDoS Attacks** (2/2)

Examples:

- **Operation Avenge Assange**
  - DDoS attacks on MasterCard, Visa, and other websites
  - cyberattack against the political decision to stop processing WikiLeaks donations
- **GitHub DDoS**
  - attack on the worldwide largest development platform on the Internet that provides source code hosting and version control for developers (now subsidiary of Microsoft)
  - maximum load: 1.3 TB **per second**

Most Common Attacks on the Internet: **Malware – Virus, Worm, Trojan** (1/2)

Malware

- **Mal**icious Soft**ware** - Software that is intentionally designed to cause damage to computers, networks, applications, services, ….

Examples (1/2):

- **Virus**
  - destructive mini-program carried by the “infected" applications or data
- **Worm**
  - malicious software that automatically spreads over open network connections
- …

Most Common Attacks on the Internet: **Malware – Virus, Worm, Trojan** (2/2)

Malware

- **Mal**icious Soft**ware** - Software that is intentionally designed to cause damage to computer, network, application, service, ….

Examples (2/2):

- **Trojan**
  - malware unintentionally installed on computer systems by a naive user
  - its functionality differs from what the user expects, e.g., installation of a backdoor or record password entries in the background, e.g.
    - "**Emotet**" is used in recent major attacks to capture financial account details

Most Common Attacks on the Internet: **Spoofing and Phishing** (1/2)

Spoofing

- Attacker sends messages with a fake sender address, e.g., fake IP address or email address. For example:
  - **CEO fraud**:
    Fake CEO instructs accounting department to send a payment to unknown banking account

Spoofing is often used in connection with:

Phishing

- "social engineering" method that asks users to reveal their sensitive information, such as passwords
- attackers use fake emails, websites, phone calls, ...

Most Common Attacks on the Internet: **Spoofing and Phishing** (2/2)

Example:

- A **spoofed email** with false sender address invites the users to access fake online banking or Facebook websites that bears a strong resemblance to the real one
- The users are prompted to enter personal data, e.g. user name, password, credit card number, etc. (**Phishing**) ...

Most Common Attacks on the Internet: **Defacement** (1/2)

Defacement

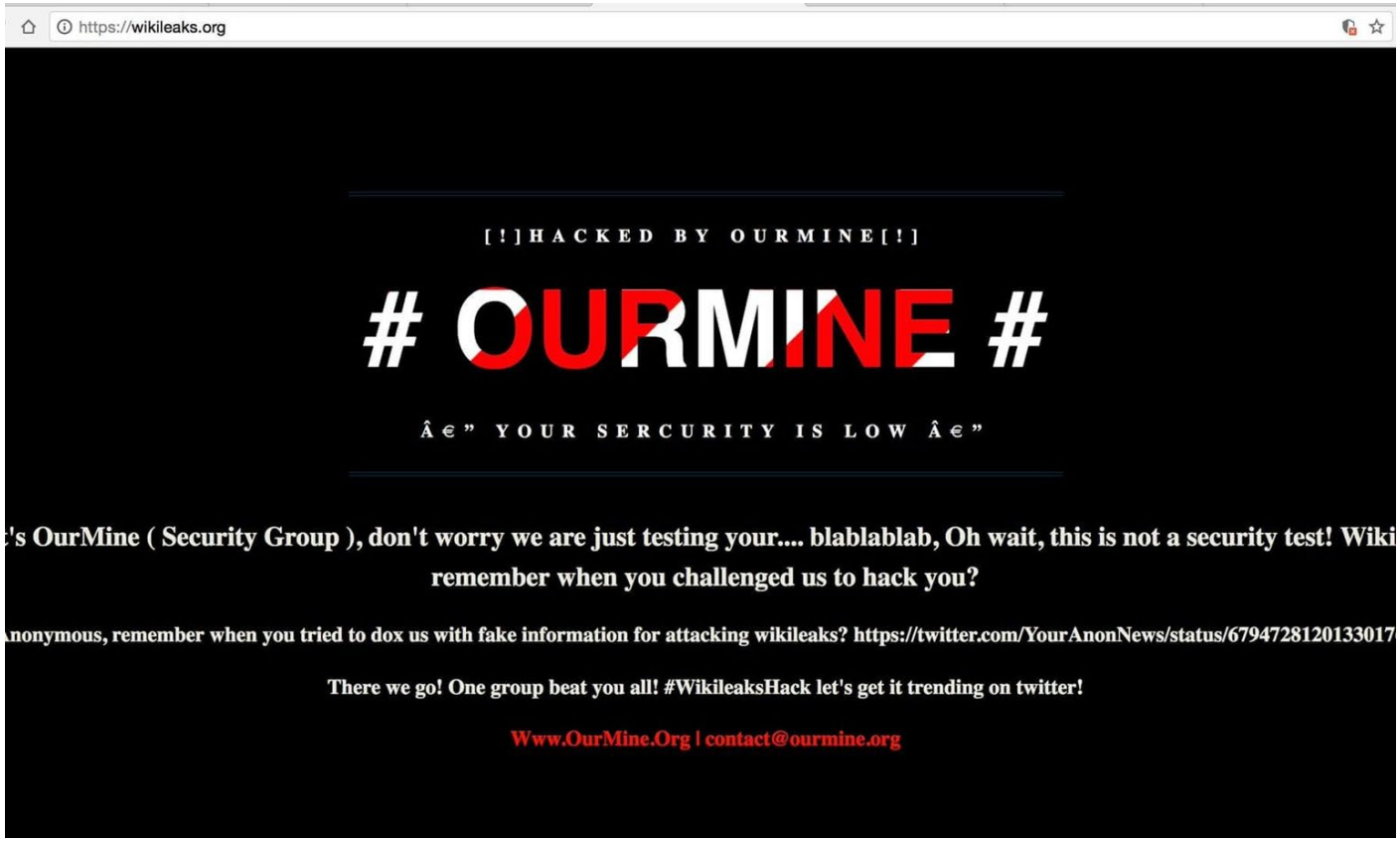
Attack on a website or web server with the intention to changing its content (De-face = changing the face)

Used for …

- Self-promotion of hacking groups, embarrassment of serious services, ...
- Attack on service availability
- **Phishing of user data**:
  - users don’t realize that the website is an unauthorized fake
  - attackers can obtain sensitive personal data, such as passwords, credit card numbers, ...

Most Common Attacks on the Internet: **Defacement** (2/2)

Example: Defacement of Wikileaks (2017) by a hacker group called OurMine



Most Common Attacks on the Internet: **Sniffing and Eavesdropping**

Sniffing is a method developed for network diagnostics by "listening" on the complete network traffic

- Administrators can use it to detect errors in the network traffic, e.g., using network sniffing software: ***Wireshark***

Eavesdropping refers to unauthorized sniffing – "listening" – to data packets on their way through the network

- Attacker connects to the victim's network while collecting and analyzing IP packets to capture personal data or other confidential private data
- Direct reading of unencrypted data traffic
- Encrypted data traffic can be recorded and decrypted later

Most Common Attacks on the Internet: **Further Attacks on Computer Systems**

- Unauthorized physical access to computer system, e.g.
  - theft of laptops, smartphones, ...
  - breaking into server rooms
- Social Engineering Attacks
  - ... not only to steal passwords like in the example of phishing
- Attack to decrypt personal data
  - password cracking
  - password guessing