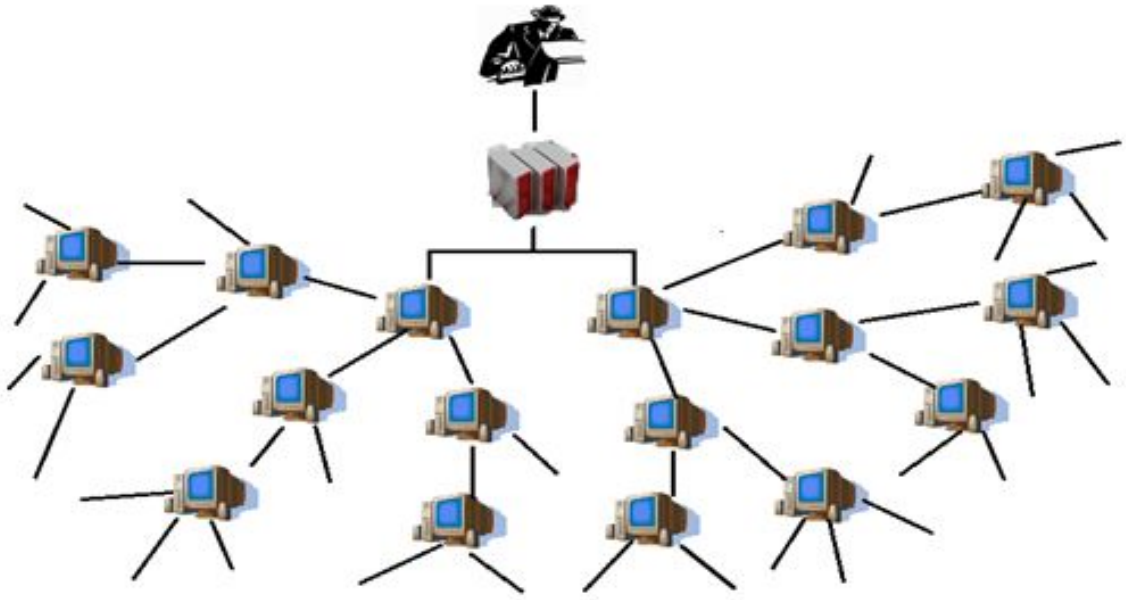
CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

Computer Security Principles

Lecture 5: Malware – Botnets & Rootkits

What is a Botnet?

- A botnet or robot network is a group of computers running a computer application controlled and manipulated only by the owner or the software source.
- A botnet may refer to a legitimate network of several computers that share program processing amongst them.



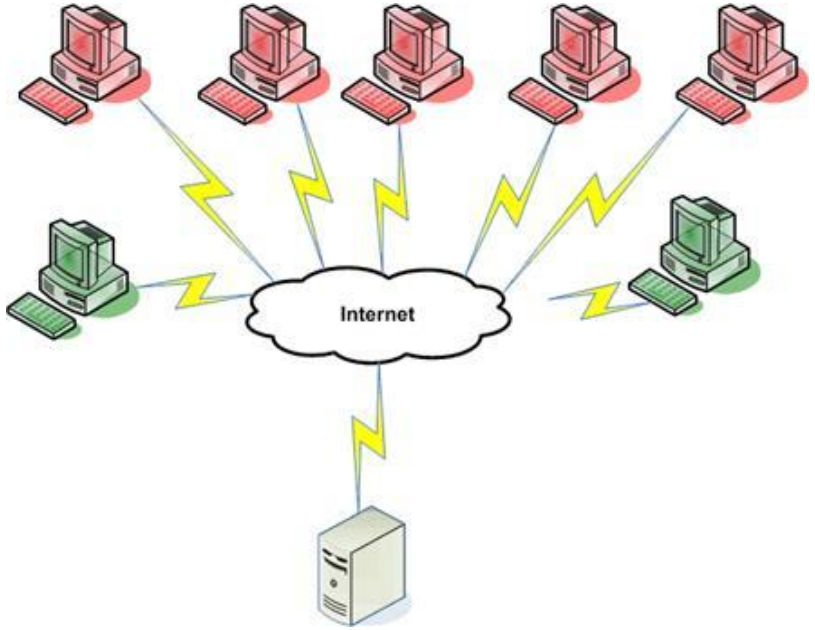
What is a Botnet?

- Usually → group of computers infected with the malicious kind of robot software, the bots
- Once the robot software has been successfully installed in a computer → this computer becomes a zombie or a drone
- Large botnet → >5,000 bots
- Small botnet → <5,000 bots
- Usually, the owners of the zombie computers do not know that their computers are bots

Potential Uses of Botnets

Distributed Denial-of-Service Attacks

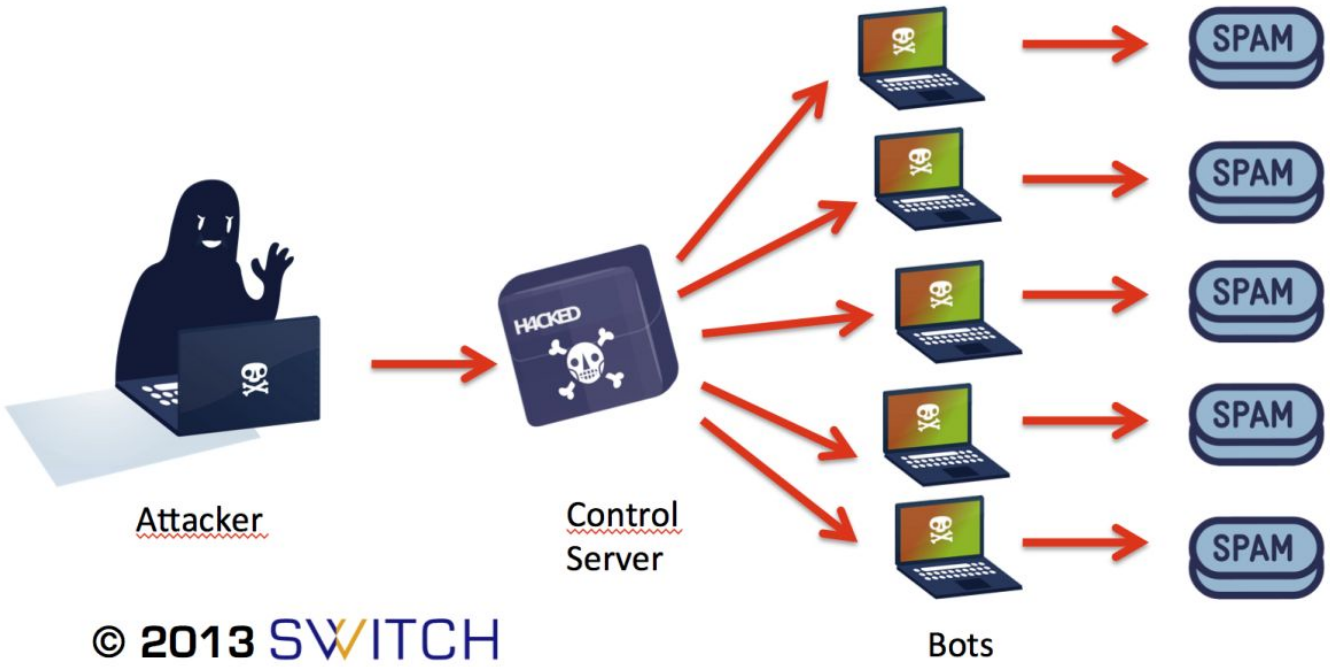
- DDoS attack is an attack on a computer system or network that causes a loss of service to users.
- Typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.
- Most commonly implemented and also very often used are TCP SYN and UDP flood attacks.



Potential Uses of Botnets

Spamming

- Thousands of bots → massive amounts of bulk email (spam).
- Can also harvest email-addresses.
- Often an old Windows computer sitting at home is the bot.
- Also used for phishing-mails (special case of spam)



Potential Uses of Botnets

Sniffing Traffic

- Packet sniffer → watch for interesting clear-text data passing
- Mostly used to get information like usernames and passwords.
- If a machine is compromised more than once and also a member of more than one botnet, the packet sniffing allows to gather the key information of the other botnet.
- It is possible to "steal" another botnet.

Potential Uses of Botnets

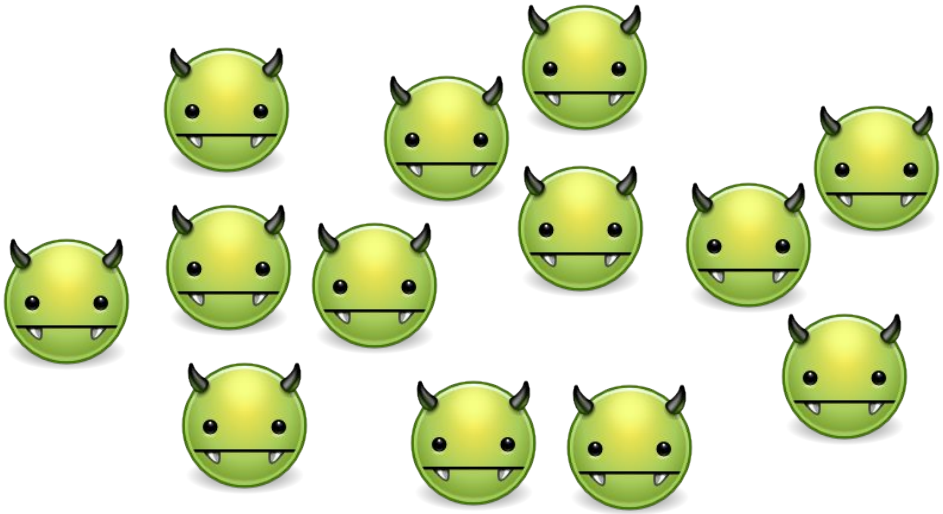
Keylogging

- Capturing of keys struck on a keyboard
- Encrypted communication channels → packet sniffing is useless, decrypt key is missing.
- Keylogger → capture info before encryption!
- Keylogger filter → capture specific data e.g. around "paypal.com"
- Keylogger on thousands of bots → paypal.com accounts quickly!

Potential Uses of Botnets

Spreading new malware

- Most common use.
- Easy → all bots implement HTTP, FTP, POP, SMTP etc.
- 10,000 host botnet → very fast spreading malware



Potential Uses of Botnets

Advertisement Addons and Browser Helper Objects

1. Negotiates a deal with some hosting companies that pay for clicks on ads
2. Set up a fake website with some advertisements
3. Botnet → "automated" clicks

Can be further enhanced if the bot hijacks the start-page of a compromised machine so that the "clicks" are executed each time the victim uses the browser.

Potential Uses of Botnets

Google AdSense abuse

- AdSense offers companies the possibility to display Google advertisements on their own website and earn money this way.
- More clicks = more money
- Botnet → "automated" click on advertisements

Manipulating online polls/games

Online polls/games are getting more and more attention and it is rather easy to manipulate them with botnets.

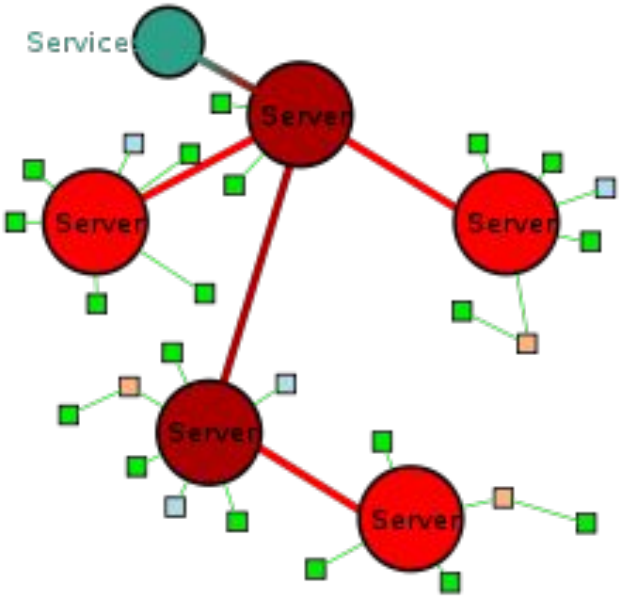
- Since every bot has a distinct IP address, every vote will have the same credibility as a vote cast by a real person.
- Online games can be manipulated in a similar way.

Potential Uses of Botnets

Attacking Internet Relay Chat (IRC) Networks

Popular among attackers is especially the so called "clone attack"

1. Controller orders each bot to connect a large number of clones to the victim IRC network
2. The victim is flooded by service request from thousands of bots or thousands of channel-joins by these cloned bots.
3. Victim IRC network is brought down - similar to a DDoS attack.



Potential Uses of Botnets

Mass identity theft

- Bots → spam emails ("phishing mails") that pretend to be legitimate (such as fake PayPal or banking emails) ask their intended victims to go online and submit their private information.
- Bots → host multiple fake websites (EBay, PayPal, banks…) and harvest personal information.
- Just as quickly as one of these fake sites is shut down, another one can pop up.
- Bots → keylogging and sniffing of traffic also

Rootkit Overview

"A rootkit is a set of programs and code that allows a permanent or consistent, undetectable presence on a computer that allows access at the most basic level to a computer's function."

Rootkits are not, in and of themselves, malicious. However, rootkits can be used by malicious programs. Understanding rootkit technology is critical if you are to defend against modern attacks.

Rootkit Actions

- Many rootkits can hide files and directories.
- Other features in a rootkit are usually for remote access and eavesdropping.
- Rootkits are not inherently "bad", and they are not always used by the "bad guys".
- There are plenty of legitimate commercial programs that provide remote administration and even eavesdropping features and some even use stealth.
- Large corporations also use rootkit technology to monitor and enforce their computer-use regulations.

Understanding Attacker's Motives

- A **backdoor** in a computer is a secret way to get access.
- Breaking into a computer system is hard work → keep the door open
- May also use the hacked computer to launch deeper attacks into the network
- Intelligence gathering needs a backdoor → keystroke capture, observe behaviour, sniff packets from the network
- May also wish to set a **logic bomb** → piece of malware that destroys the system when certain conditions are met

Why do Rootkits exist?

Rootkits provide two primary functions:

- **Remote Command and Control:** control over files, causing reboots or "Blue Screens of Death," and accessing the command shell (that is, cmd.exe or /bin/sh).
- **Software Eavesdropping:** sniffing packets, intercepting keystrokes, and reading e-mail, capture passwords and decrypted files, or even cryptographic keys.

How do Rootkits work?

- Rootkits work using a simple concept called **modification**.
- In general, software is designed to make specific decisions based on very specific data.
- A rootkit locates and modifies the software so it makes incorrect decisions.
- There are many places where modifications can be made in software. Some examples:
  - Patching
  - Easter Eggs
  - Spyware Modding
  - Source Code Modding

How do Rootkits work?

Patching

- Executable code consists of a series of statements encoded as data bytes → these bytes come in a very specific order
- Modify bytes → modify software logic
- Technique used to remove software protections

Easter Eggs

- "built in" → programmer places a hidden back door in a program

Spyware Modifications

- Sometimes a program will modify another program to infect it with "spyware."

How do Rootkits work?

Source Code Modification

- Sometimes software is modified at the source—literally.
- Programmer can insert malicious lines of source code into a program
- Reason some militaries use separate Linux fork
- Main Linux distros → open-source projects, almost anyone can add code

Defending against Rootkits

Same prevention as other malware:

1. Keep systems patched.
2. Cover all the infection vectors (e.g., email attachments, Web downloads, removable media) with antivirus technologies and keep the signatures up to date.
3. Refrain from engaging in dangerous activities → torrent sites, cracked software etc.
4. Disable unneeded features and services; don't install unneeded applications.

Rootkit Defences - Detectors

Linux

- Chkrootkit - www.chkrootkit.com
- Rootkit Hunter - www.rootkit.nl/projects/rootkit_hunter.html

Windows

- Rootkit Revealer - www.microsoft.com/technet/sysinternals
- F-Secure's Blacklight
- ICE Sword
- Sophos Anti-Rootkit
- McAfee Rootkit Detective
- Patchfinder

Rootkit Defences – File Integrity Checkers

- Look for changes to critical system files
- Although if the attacker is very careful and covers their tracks, they can fool the file integrity checker
- Tripwire and AIDE are classic tools which can be used.
- Tripwire maintains an encrypted database of file checksums so it can detect system changes which may indicate a compromise.

Defences – Booting

- When a kernel-mode Rootkit is suspected, you cannot trust anything the kernel is telling you about the system.
- Solution – Toss out the kernel and investigate with trusted tools
- Boot from a Linux CD-ROM designed for incident response and digital forensics
  - CAINE - http://www.caine-live.net/
  - SIFT - http://digital-forensics.sans.org/community/downloads
  - X-Ways - http://www.x-ways.net/forensics/