

BotNets

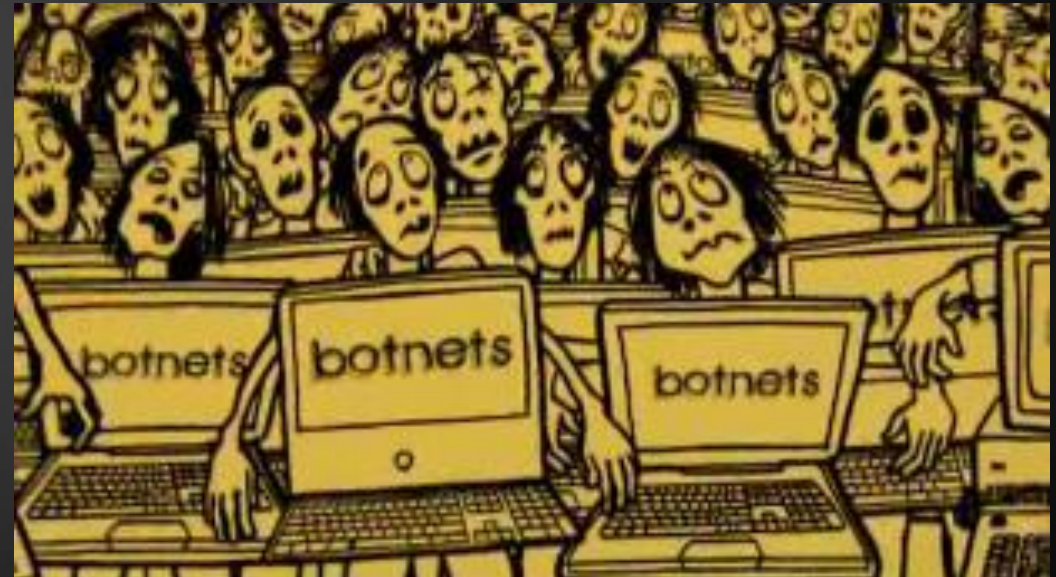
Hüseyin Yağcı



Outline

2

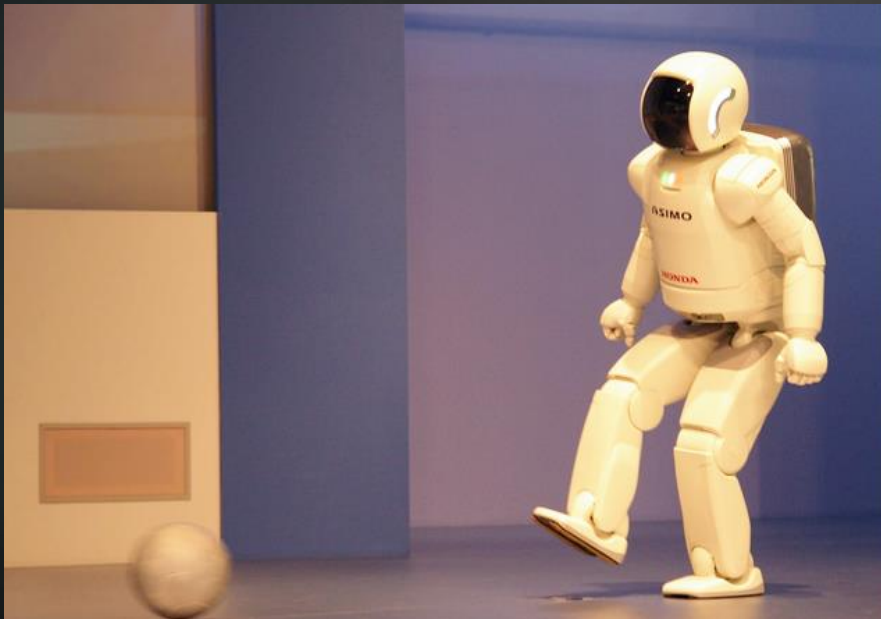
- ▶ Introduction - History
- ▶ Detection & Defense techniques
- ▶ Motivational attacks




Introduction - History

3

- ▶ Word of bot comes from robot, means capable of carrying out a complex series of actions automatically. *
- ▶ Bots are using in many fields of computation. Nowadays, AI powered bots running for correcting our mistakes and maintaining the order of internet.



 **ComputeBot** BOT 4:40 PM Only visible to you

@matt asked to compute **meaning of life**. Hold tight...

Result (2KB) ▾

42
(according to the book *The Hitchhiker's Guide to the Galaxy*, by Douglas Adams)

[Learn More on WolframAlpha](#). Try this yourself with /compute.

@matt asked to compute **population of earth**. I'm on the case...

Result (1KB) ▾

7.28 billion people (2015 estimate)

Population (3KB) ▾

population	7.28 billion people (2015 estimate)
population density	118 people/mi ² (people per square mile)

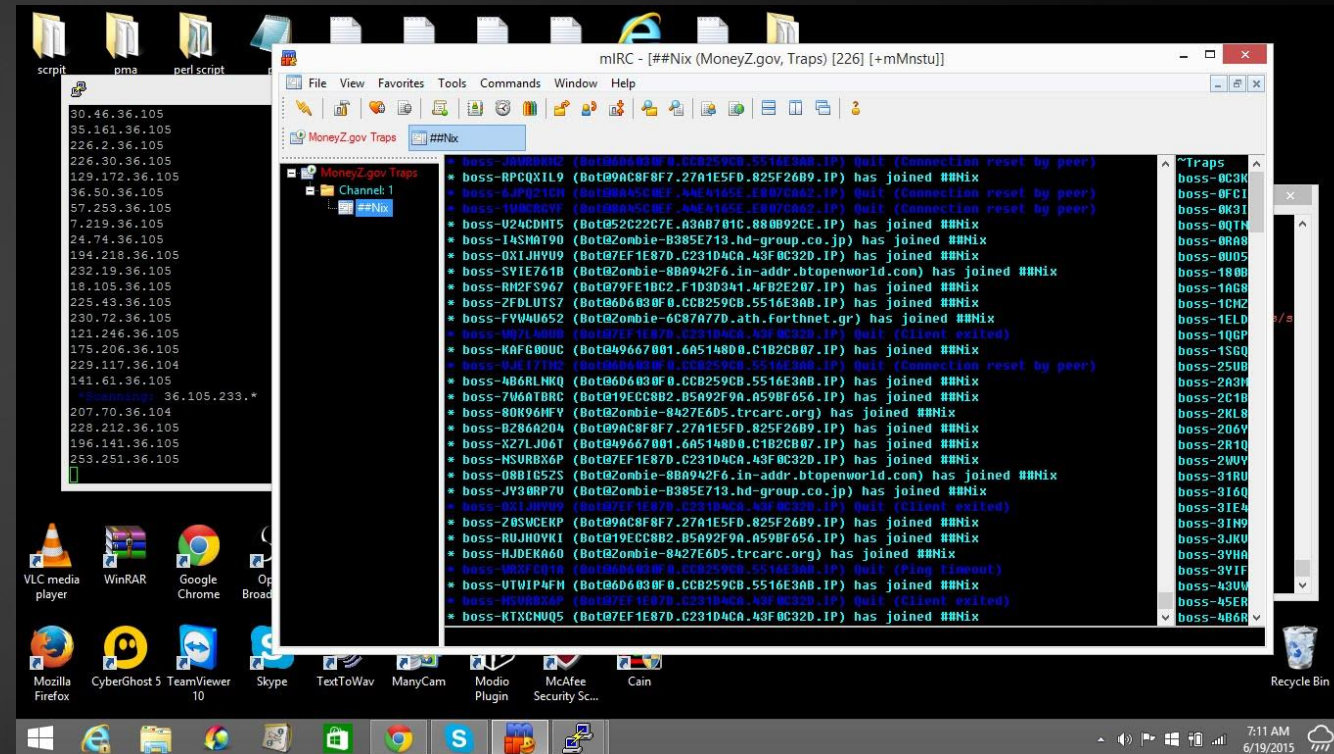
[Learn More on WolframAlpha](#). Try this yourself with /compute.

* <https://www.honeynet.org/papers/bots>

Introduction - History

4

- ▶ Botnet principles starts with harmless usage of bots in Internet Relay Chat (IRC) channels. For security purposes.
- ▶ First IRC bot Eggdrop, was published in 1993. *
- ▶ GTbot and its variants is considered as the point from which botnets became a major threat to the internet.*



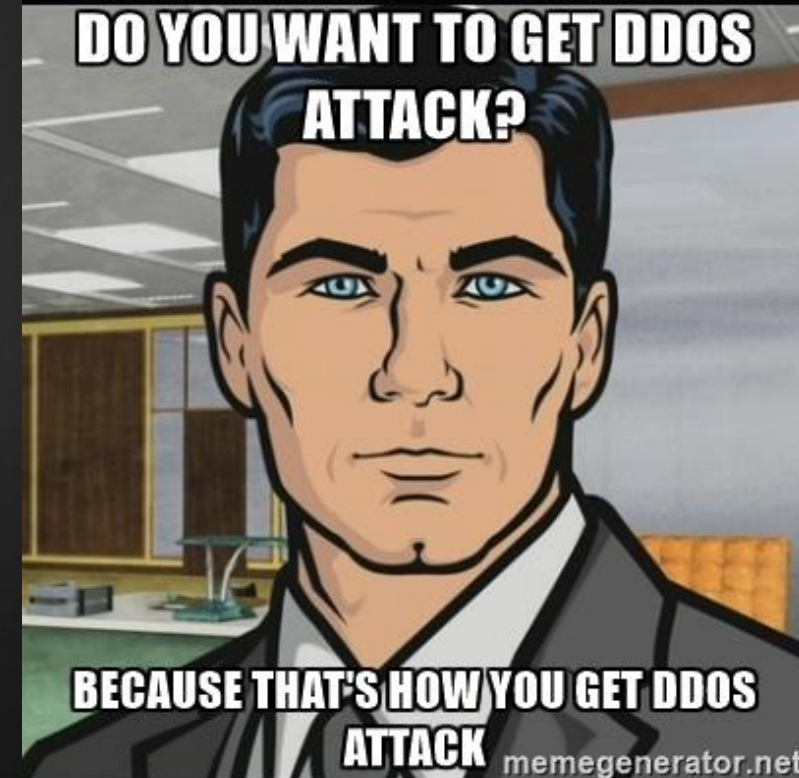
- <https://www.eggheads.org/>
- **Development of GTBot, a high performance and modular indoor robot**, G. Macesanu, T. T. Coda, C. Suliman, B. Tarnauca.

Introduction - History

5

- ▶ Botnet starts with the conception of developer.
 - ▶ Motivations of botmaster have been classified as money, entertainment, ego, entrance to social groups and status.*
 - ▶ Mostly motivations are related to financial gain.

• Symantec global internet security threat report trends of 2009. Tech. Rep. DIY kit of Turkojan, Symantec. TURKOJAN



Introduction - History

6

- ▶ Design *
 - ▶ Command and control server communication.
 - ▶ Botnet architecture can be centralized, distributed or hybrid.



* Survey and Taxonomy of Botnet Research Through Life-Cycle, Rafael A.R, Gabriel M.F, Pedro G.T, University of Granada

Introduction - History

7

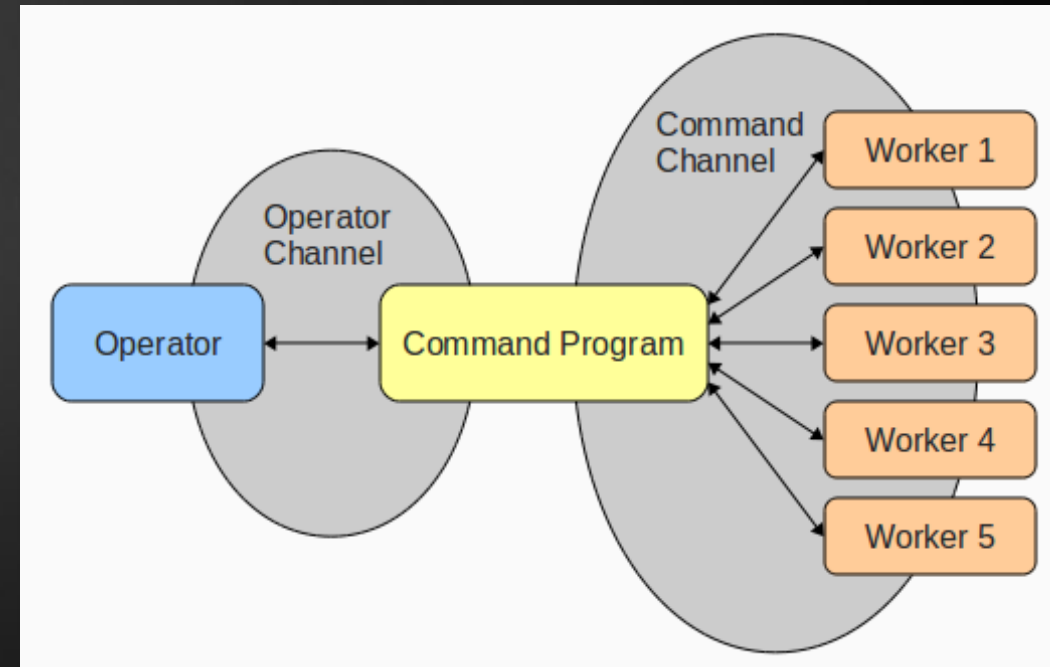
- ▶ Recruitment
 - ▶ Implemented Botnet software must be deployed for operation in a real environment.
 - ▶ Recruitment, also known as infection, has been widely studied in literature.
 - ▶ Binary exploitation
 - ▶ Unreported bugs (zero-days)
 - ▶ Reported bugs (exploitable programs)
 - ▶ Brute force
 - ▶ Social engineering



Introduction – History

8

- ▶ Interaction
 - ▶ Refers to all the interactions performed during the botnet operation,
 - ▶ The orders sent by botmaster.
 - ▶ Messages interchanged between bots.
 - ▶ External communications from the botmaster to monitor Botnet information.
 - ▶ The communications of bots with external servers.



Introduction – History

9

- ▶ Marketing

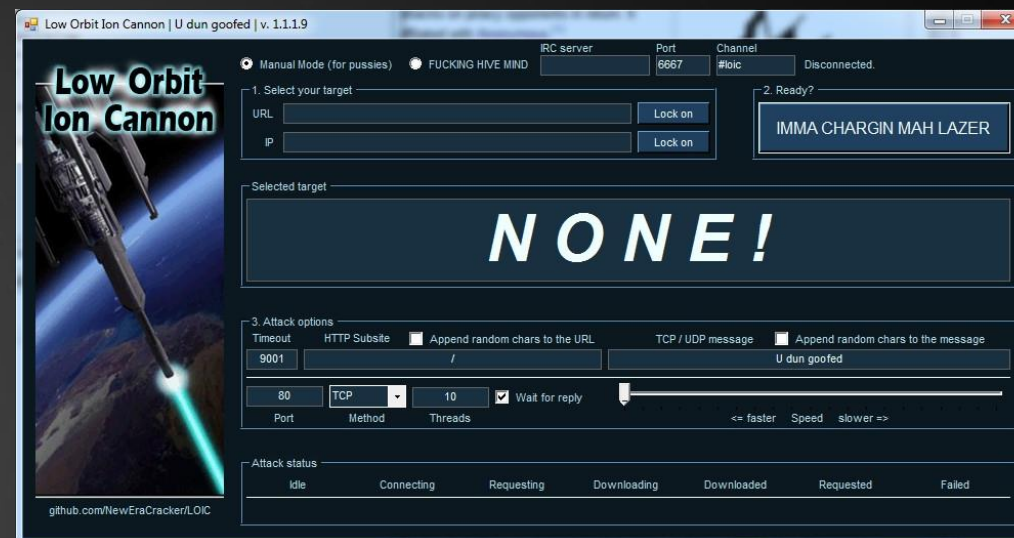
- ▶ Selling source code. DIY kits. *

- ▶ Zeus Botnet kit

- ▶ Turkojen

- ▶ Services to be rented.

- ▶ Distributed Denial of services DDoS attacks, email addresses, spam mail services, user accounts, fast-flux networks, search engine spam



* Another pleads guilty in Botnet hacking conspiracy. Tech. Rep., FBI Press Release. June [2010]

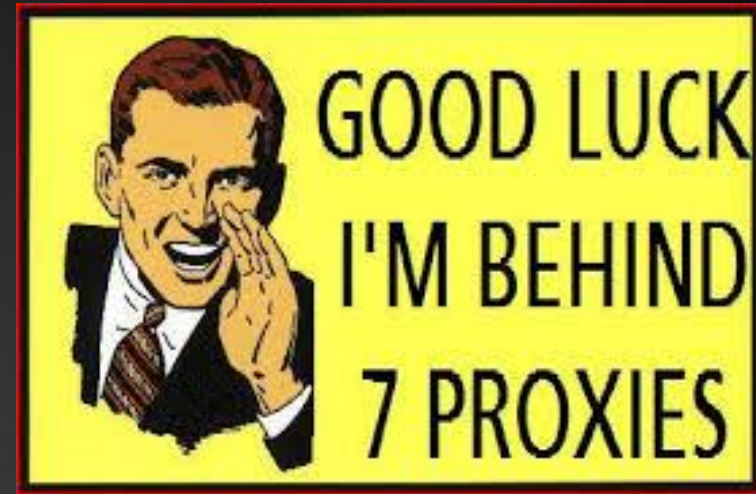
Introduction – History

10

- ▶ Attack execution
 - ▶ DDoS
 - ▶ Spamming
 - ▶ Phishing
 - ▶ Data stealing
 - ▶ Click fraud

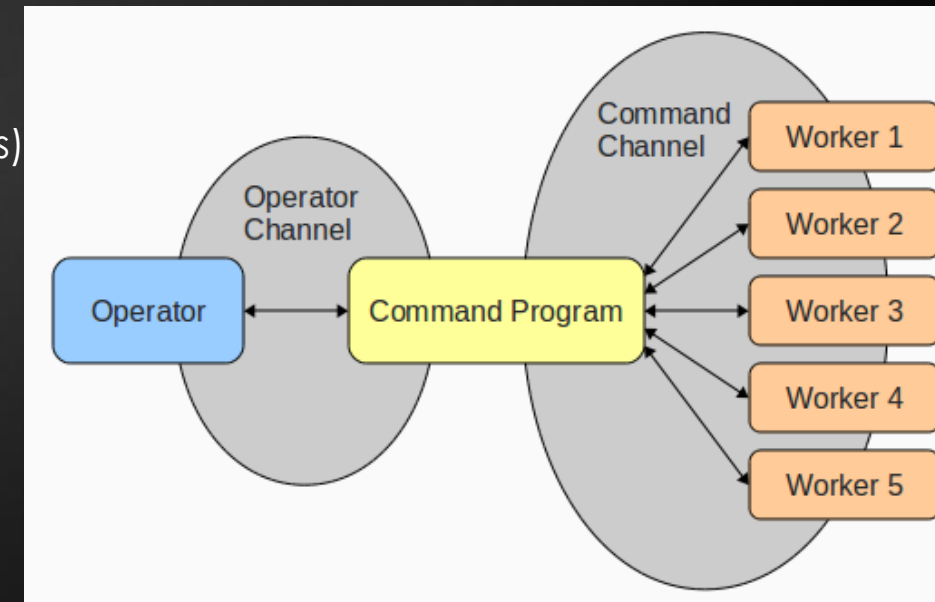


Introduction – History



11

- ▶ Complementary Hiding Mechanisms
 - ▶ Multiple proxies;
 - ▶ Hiding communication between C&C and bots.
 - ▶ Cipherring;
 - ▶ Communication encryption mechanisms.
 - ▶ Binary obfuscation;
 - ▶ Conceal the source code of bot (Anti reverse techniques)
 - ▶ Polymorphism;
 - ▶ Creating different versions of the source code of a program, which change while its functionality remains unaffected.
 - ▶ IP, Email spoofing



Introduction – History

12

- ▶ Complementary Hiding Mechanisms v.2
 - ▶ Domain name Generation Algorithms (DGA); *
 - ▶ That are used to periodically generate a large number of domain names that can be used as rendezvous points with their command and control servers.

```
x = rand(10)

domain = "xyz" + x + ".com"

contact(domain)
```

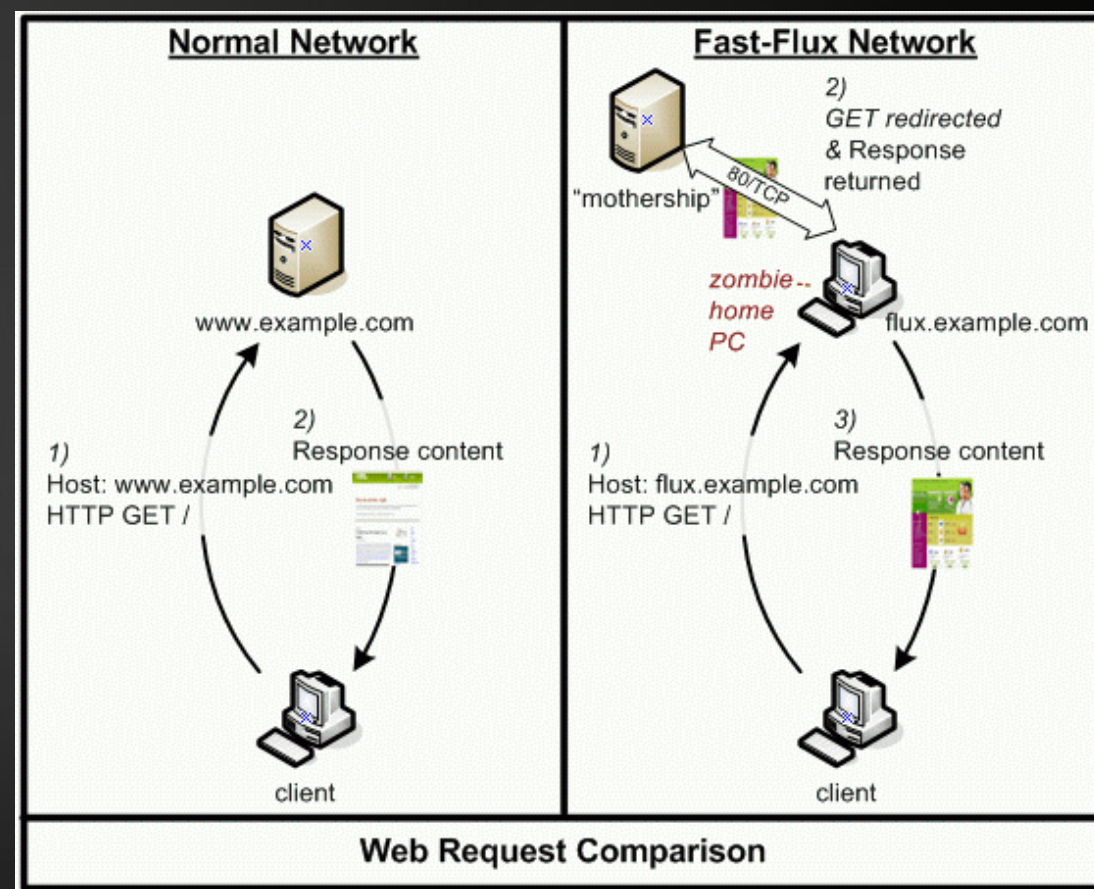
* https://en.wikipedia.org/wiki/Domain_generation_algorithm

Introduction – History

13

- ▶ Complementary Hiding Mechanisms v.3
 - ▶ Fast-Flux networks; *
 - ▶ The goal of fast-flux is for a fully qualified domain name (such as `www.example.com`) to have multiple (hundreds or even thousands) IP addresses assigned to it.
 - ▶ These IP addresses are swapped in and out of flux with extreme frequency, using a combination of round-robin IP addresses and a very short Time-To-Live (TTL) for any given particular DNS Resource Record (RR).

* <https://www.honeynet.org/node/132>

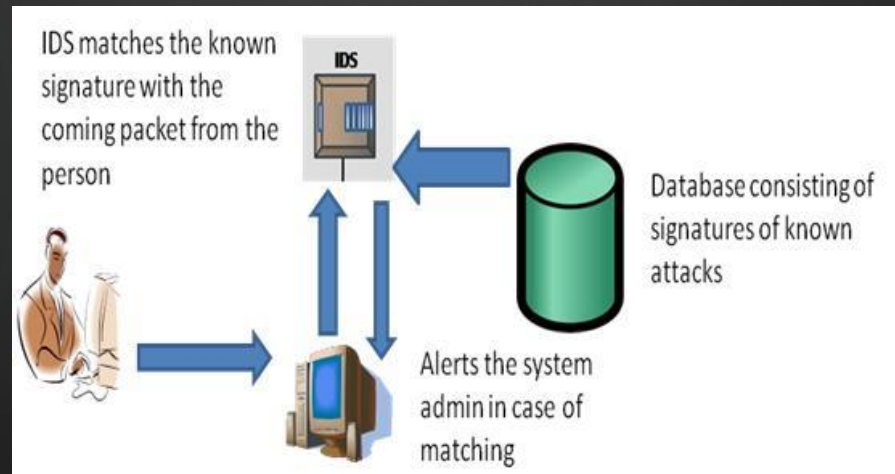
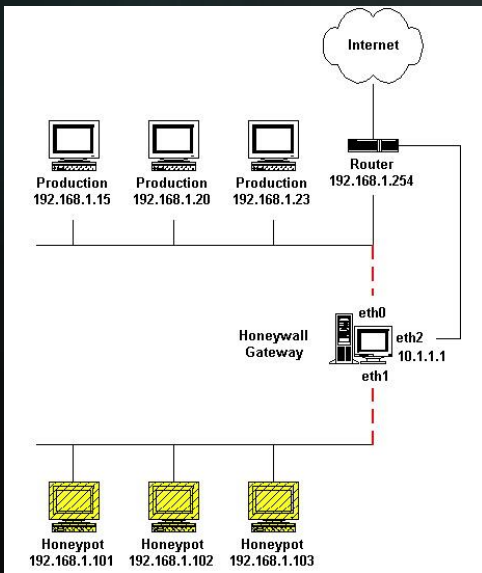


Detection & Defense techniques

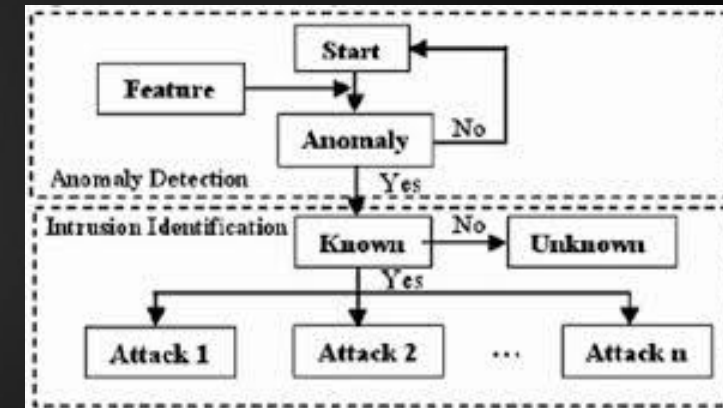
14

- ▶ Classified into two main categories;
 - ▶ 1 Setting up honeynets
 - ▶ 2 Intrusion Detection systems (IDSs).
 - ▶ 2¹ Signature based
 - ▶ 2² Anomaly based

1



2.1

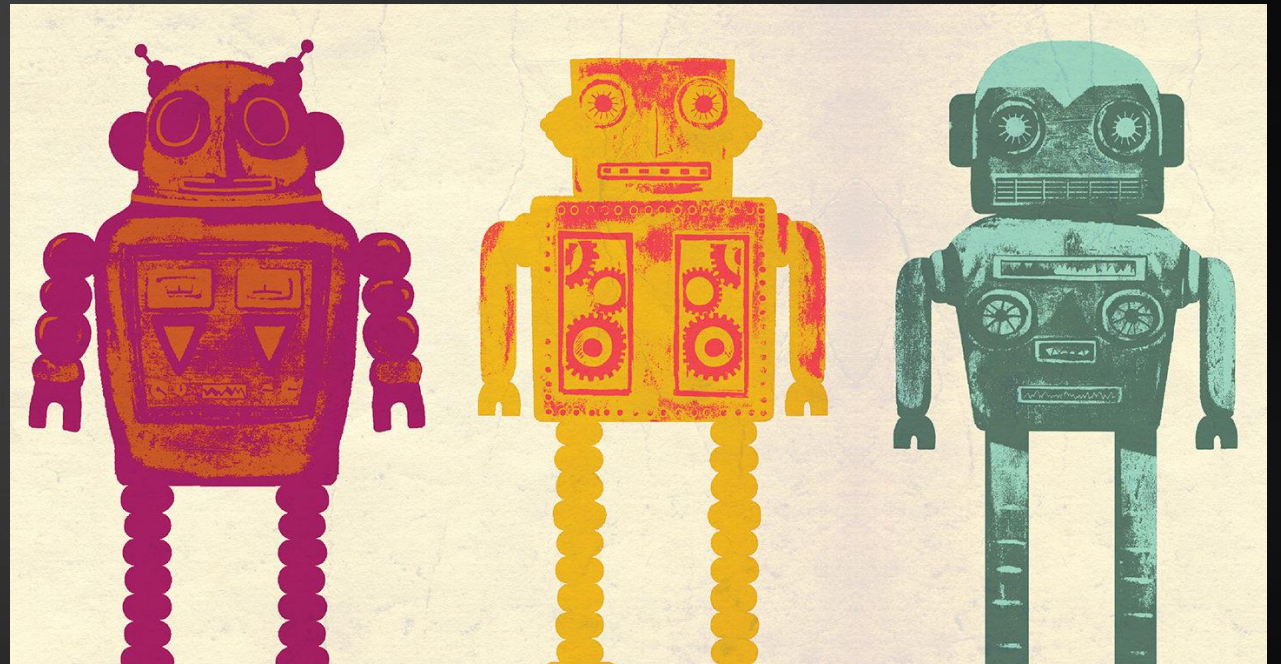


2.2

Motivational attacks

15

- ▶ Grum [2012]:
 - ▶ Responsible for up to **26%** of the World's spam email traffic.
- ▶ Conficker [2008]:
 - ▶ 10M
 - ▶ P2P, decentralized
- ▶ Zeus [2007]:
 - ▶ Allows the creation of new bots
 - ▶ More than 3000 variants



Motivational attacks

16

- ▶ Mirai [2016]:
 - ▶ First Internet of Things (IoT) Botnet. 1.2m device
 - ▶ Opensource.
 - ▶ GitHub, Twitter, Reddit, Netflix, Airbnb



THANK YOU