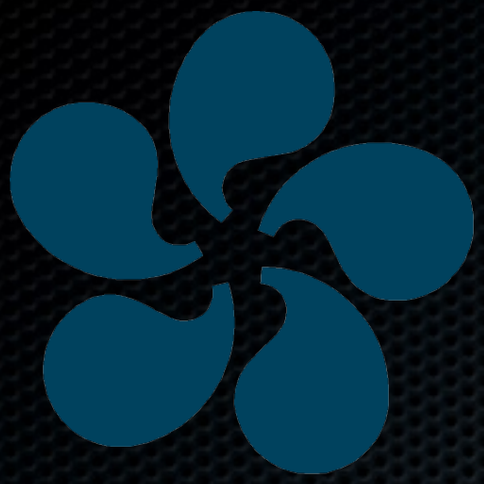


IPN lis

CERT-IPN COMPUTER SECURITY INCIDENT RESPONSE TEAM

Spam-Fighting

Workshop CNSA-LAP

7, October, 2009

Lisbon, Portugal

Botnet Tracking

Francisco Nina Rente

Agenda

- Presenting CERT-IPN
- Botnet: What, how and where?
- Historical perspective
- Real Cases: International
- Real Cases: National
- Defense Measures
- Conclusions

CERT-IPN

CERT-IPN is a **CSIRT** (Computer Security Incident Response Team), integrated in the Computer Science Laboratory (**IPNIis)** from Pedro Nunes Institute (**IPN**), whose mission statement is "**Bringing Security to the Portuguese's Information**".

http://www.cert.ipn.pt

CERT-IPN core activities:

(1) Dissemination Services

(2) Consulting Services

(3) Business Continuity support Services

certIPN ©

CERT-IPN

Consulting Services

http://www.cert.ipn.pt/pt/consultoria.html
http://www.cert.ipn.pt/en/consulting.html

- Penetration Tests
- Systems and Network Security Assessment
- Security and Robustness Application Assessment
- Consulting and Designing of Information Security Solutions
- Forensics Analysis and Data Recover
- Workshops and Training in InfoSec

CERT-IPN

Dissemination Services

http://www.cert.ipn.pt/pt/disseminacao.html
http://www.cert.ipn.pt/en/dissemination.html

- Security Incident Response

  Constituency – Ipv4 addresses from IPN

- InfoSec awareness and dissemination

Vulns PT
> setSafe(vulnerabilidade);

Talks, Conferences, Workshops, Digital Publication, Training...

- Collaboration with Portuguese Security related Projects

TRUSTED Introducer

enisa European Network and Information Security Agency

The Honeynet Project Portugal

Nonius

certIPN ©

Botnet
What, how and where?

To tune up

- Botnet: networks of **compromised machines,** remotely **controlled** by an attacker, used to conduct several **attacks**
- Bot: **compromised machine**, used within a botnet
- Attacks (most popular): DDoS, SPAM, Phishing and massive identity theft

Botnet

What, how and where?

What are Botnets?

Technical Perspective

- Modifiable and extensible software (malware)
- Conceptual Hierarchical organization
- Redundant and robust networks

Social Perspective

- “Weapons of mass destruction”
- Organized crime newest toys
- Government newest weapons

Botnet

What, how and where?

How?

Where?

Internet connected machines (not only the facing ones!)

Historical perspective

- **Worm concept** appeared with Robert Tappan Morris in late 80's – Morris Worm
- **IRC protocol** approved in 1993 (RFC 1459)
- Early to Mid 90's malware starts to add **automated IRC functionality** (communication, updates...)
- Late 90's – began to use **remote exploitation** to public/private network conquest

Historical perspective

Basic needs for Communication

in late 90's

Historical perspective

Begin of 21 century

- Cryptographic, obfuscation, polymorphic and packing abilities
- Modular design; counterattack and proactive defense (disabling A.V., Firewall...)
- P2P Networks – non centralized networks
- All sort of malware capabilities – spyware, rootkits, adware...

Historical perspective

Robust Communication

Strong “weapons”

Stealth abilities

in the beginning of the 21 Century

Historical perspective

2007 – Storm Worm

2008 – Conficker

Intelligence

Decision capabilities based in:

- user behavior
- machine and network status

Real Cases: International

- **Estonia, April 2007**: Several massive attacks were carried out against the main Estonian organization (Government, Military, Banks...). Attacks from DDoS to SPAM and defacements, were made using botnets.

- **Jihad Botnet –** In late 2007, it was a big hype in the community, based in a set of rumors about a malware specimen implemented by Jihad aiming to build a botnet.

Real Cases: International

- **Georgia, August 2008:** Government and other Critical infra-structures were the target. DDoS attacks were carried out supposedly by several Russian botnets.

- **Ghostnet, March 2009** - large-scale cyber spying operation discovered infiltrated high-value political, economic and media locations in 103 countries (including Portugal). Supposedly with Chinese origins. Supported by a “dumb” botnet based in a open source proof-of-concept malware.

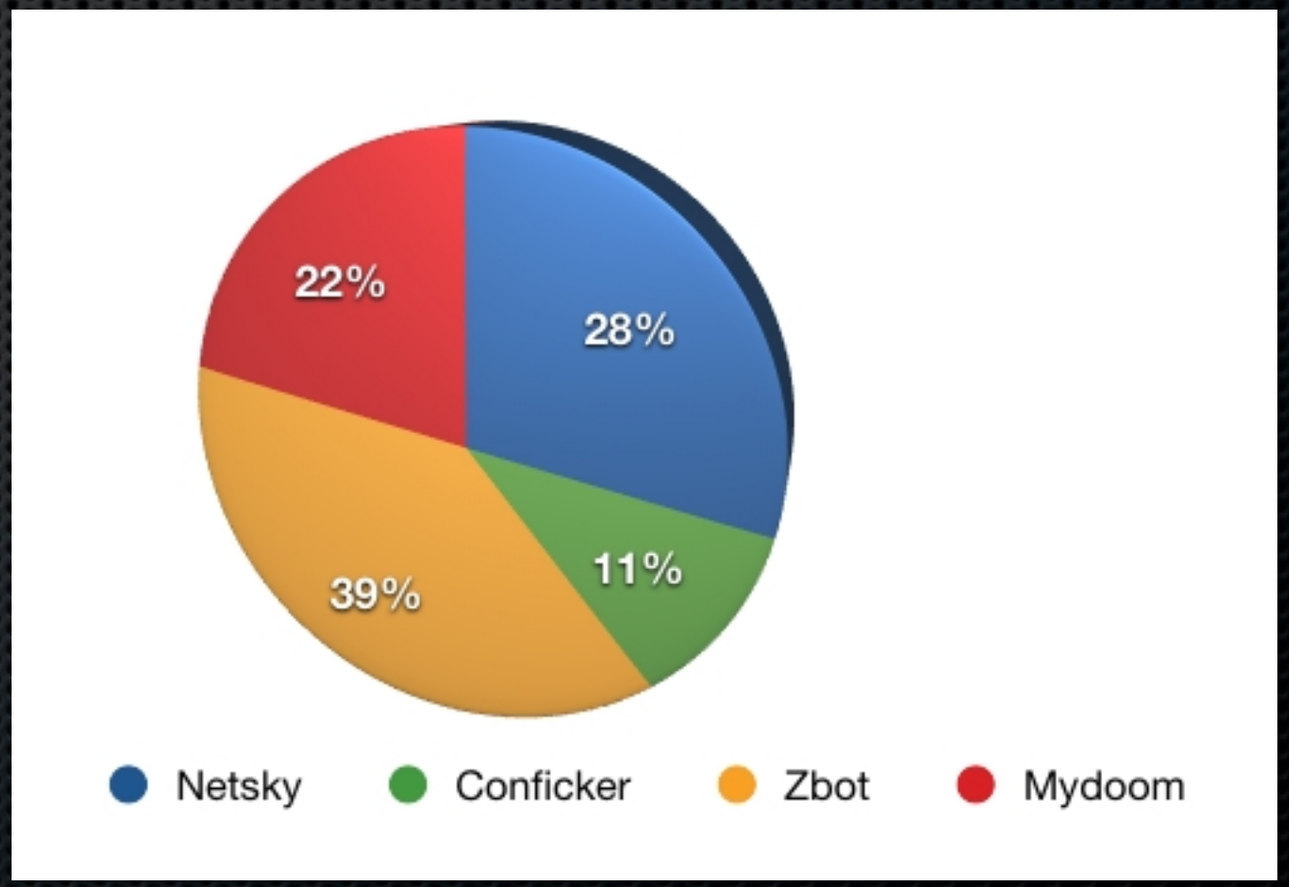
Real Cases: National

- ZEUS Botnet (ZBot) - Millennium BCP in the Top10 of phishing targets (by Clemens Kurtenbach in HAR2009)

- Data gathered by CERT-IPN:
  - Project Nonius
  - Honeynet (ISPs: Vodafone, Vodafone ADSL, Zon/Netcabo, SAPO ADSL and MEO)

August 2009

-/+ 5k active bots



Defense Measures

	Type	Objective
C&C	Pro-active Defense	Disable/destroy botnet control center.
Update System	Pro-active Defense	Disable/destroy botnet update/synchronize capabilities.
Communication channel	Defense	Analise and define filters. Understand cover channel techniques.
Honeypot	Study	Understand and map the botnet resources, behavior and organics
Darknet	Study	Understand and map the botnet resources, behavior and organics

Conclusions

- Botnets **aren't a new** threat
- Nowadays, botnets use the **cutting edge technologies**
- Botnets start being used as **war weapons**, **profit mechanisms**, massive **organized crime** support

Curiosity: The three most active botnets, sent 21 Billion spam mails daily -- Symantec, August 2009

Conclusions

- IRC based botnets are still the most used
- Two types of defenses: **pro-active and passive**
- **Understanding** (studying) botnets is very **important**. Defense systems depend on it.
- Portugal participation in this “crime game” is mostly as pawns.

Thank you for your attention.

Q & A

IPN lis

CERT-IPN COMPUTER SECURITY INCIDENT RESPONSE TEAM

www.cert.ipn.pt

certIPN ©