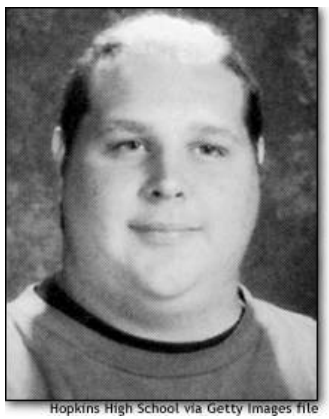
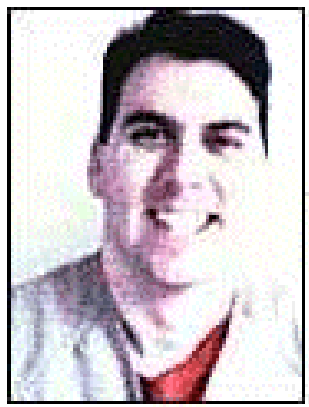
New Threats evolution

David Sancho
TrendLabs Av-EMEA

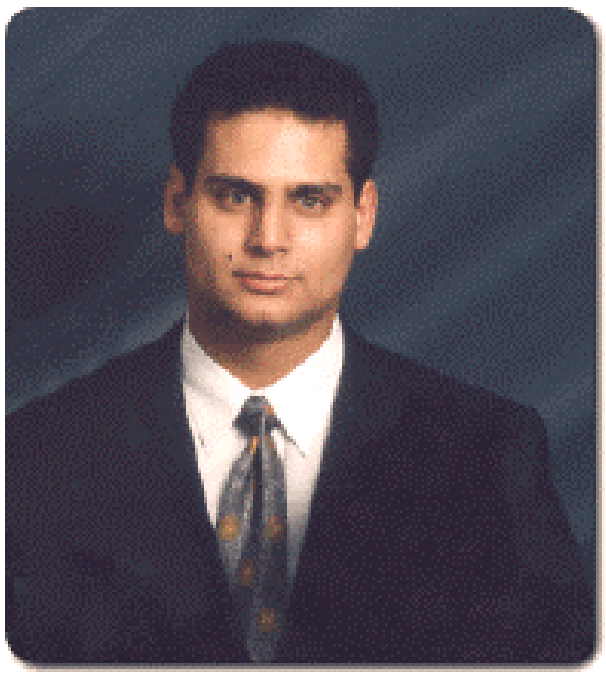
Old enemies





New enemies

Jay R. Echouafni



Jeremy D. Janes

Andrew Schwarmkoff

Threats in 2005

- Bot worms
- Trojans
- Spyware/Grayware
- Phishing
- Pharming

Bot Worms

- Zombies: Infected PCs sleep until the attacker wakes them up

- Botnet: a network made up of zombies

Bot Worms

- What's the purpose of bot worms?
  - Get Money:

    - Selling botnet to spammers
    - Uploading spyware/adware
    - Sending DoS to websites

Recent examples include:

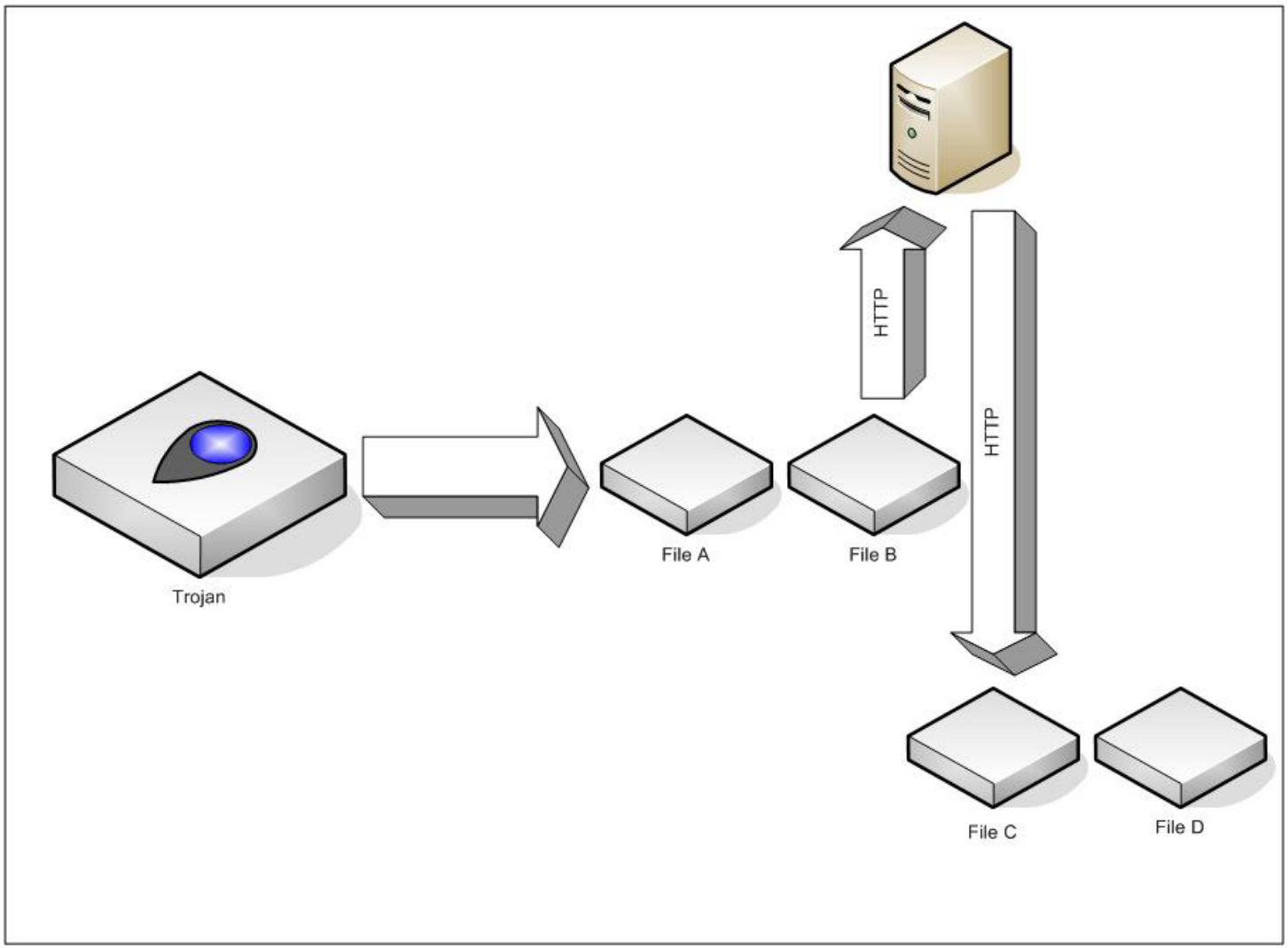
SDBOT, AGOBOT and MYTOB

Trojans

- Trojans can’t replicate by themselves.

- Downloaded by the user from some webpage

- Trojan cycle…

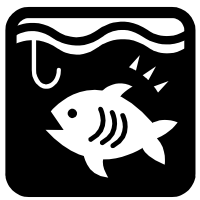


Spyware/Grayware

- Spyware/Grayware: non-malicious threats - security breaches

- Spyware comes downloaded from the web

Phishing



- Emails seem to come from a bank, asking to validate your login
- They redirect you to a fake website
- You give login data, they steal the money

Phishing

Fw: Lloyds TSB: Urgent Notice From Billing Department

File Edit View Tools Message Help

FW: Spam: Ba?l

From: Justin D
Date:
To:
Subject: FW: Sp

Dear Barclay

This email wa
on the link be
This is done f
must verify it.

http://barclay

Barclays : Privacy Policy : Personal Information (new window) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://www.barclays.com/privacy/per_info.html

BARCLAYS

Privacy Policy : Personal Information

Personal Inform
Cookies

Your E-Mail Was Verified. - Microsoft Internet Explorer

Thank you.

Your E-Mail Address Was Successful Verified.

- to credit reference and fraud prevention agencies and other organisations who may record, use and give out information to other lenders and insurers. The information may be used to make assessments for credit and all types of insurance, for debt tracing and to prevent fraud and money laundering;
- to persons acting as our agents under a strict code of confidentiality;
- to anyone to whom we transfer or may transfer our rights and duties under your Customer Agreement;
- as required by law or regulation.

Otherwise we will keep information about you confidential.

Internet

BEWARE: COPY OF FRAUDULENT PHISHING ATTEMPT

Sincerely,
Lloyds TSB Bank., Account Review Departnemt

http://lloydstsb.safeedible.net/

Pharming

- DNS Server attack
- Can redirect to fake websites
- Can redirect to spyware sites

Any Question?