



Targeted Attacks

Swa Frantzen

Brussels, 29 Oct. 2008

Introduction

- Swa Frantzen
 - swa@section66.com



Define targeted attack

Is E-mail sent to you enough ?



Attack that discriminates

common: low exposure
“fly under the radar”

Evolutions leading to targeting

- **Past**
 - **Goal:**
 - Fame
 - Cause mayhem

 - **Methods**
 - Viruses
 - Worms
 - Trojans
 - Defacements
 - ...

Evolutions leading to targeting

- **Present**
 - **Goals**
 - **Earn money**
 - **Build tools to earn money**
 - **Organized crime**
 - **Methods**
 - **Botnets (spam, DoS, extortion)**
 - **Password stealing Trojans**
 - **Banking Trojans**
 - **Drive-by downloads**
 - **...**

Evolutions leading to targeting

- **Botnet**
 - Divide it in portions
 - Divide by geo-location
- **Defacements**
 - “interesting” victims
 - Government more prestige than amateur site
 - Dolphin stadium defacement
- **Droppers**
 - Don’t give downloads to known white hats
- **Malicious iframes**
 - Hide them to search engines
 - Hide them from visitors not coming from a search engine
- **Phishing**
 - “spear phishing”

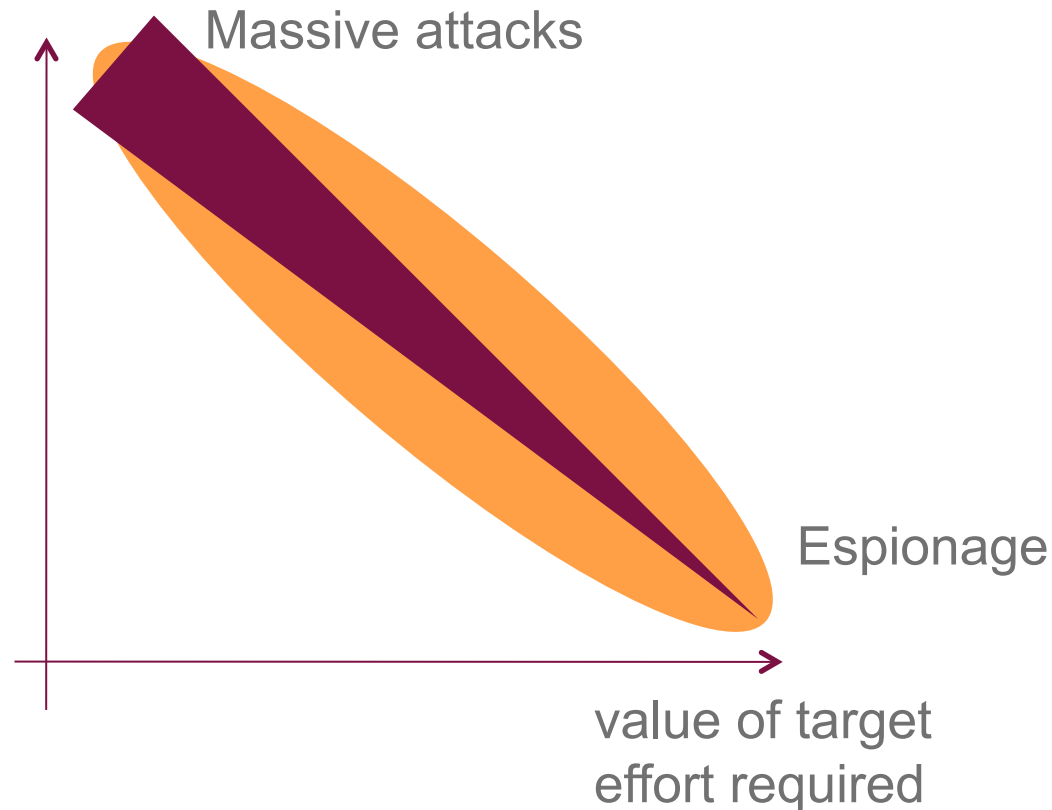
Targeted attack characteristics

- **Low profile: avoid detection**
 - Towards the victims
 - Towards the attacker
 - Towards others
- **Fewer targets ⇒ better preparation**
 - Economics
 - Chance of success needed
- **Used today already**
 - politically motivated actions
 - industrial espionage

Targeted attacks: classification

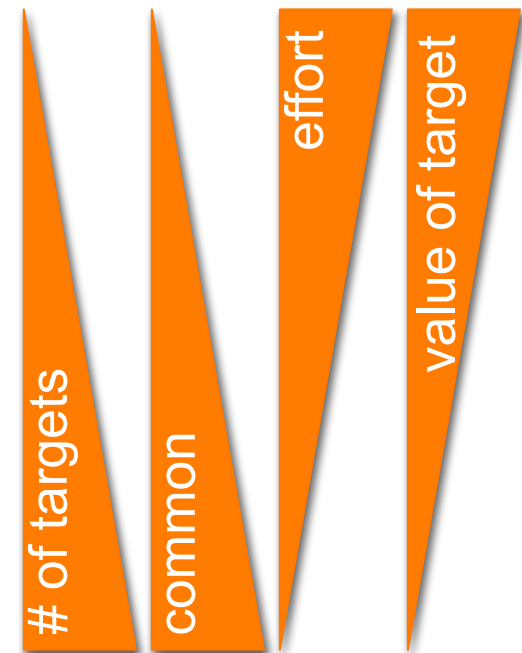
- How targeted is the attack?
- How much is it discriminating?

targets



Targeted attacks: classification

- **Pyramid of possibilities**



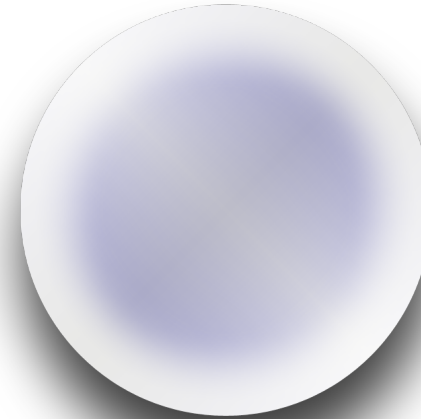
Existing defensive measures

- **Anti-virus**
 - After a while, unless you were the only recipient
- **Firewall**
 - Not much protection for client attacks
- **IDS/IPS**
 - It depends ... signature needed
 - Low profile connections are hard to find
- **Configuration changes**
 - Yes! But which?
- **Awareness**
 - A challenge, does the user have a chance?
- **Architecture**
 - We allow communication from clients

The future

Unanswered questions ...

- How fast will it grow ?
 - What level of targeting ?
- What can we do to defend against it?
 - Espionage:
 - Awareness?
 - Architecture?
 - Mass attacks:
 - Antivirus/IDS/IPS?
 - Based on behavior?



Q&A

Thanks for your attention

Contact

- **Swa Frantzen**
 - swa@section66.com
- **Internet Storm Center**
 - <http://isc.sans.org/contact.html>
- **Presentation**
 - <http://www.section66.com/security/isaca2008.pdf>