

The background features a red field with five yellow stars in the upper left, arranged in an arc. The rest of the background is filled with a complex, abstract pattern of overlapping, wavy lines in shades of red, orange, and yellow, resembling a dragon's scales or a traditional Chinese motif.

The snooping dragon:

**social-malware surveillance of
the Tibetan movement**

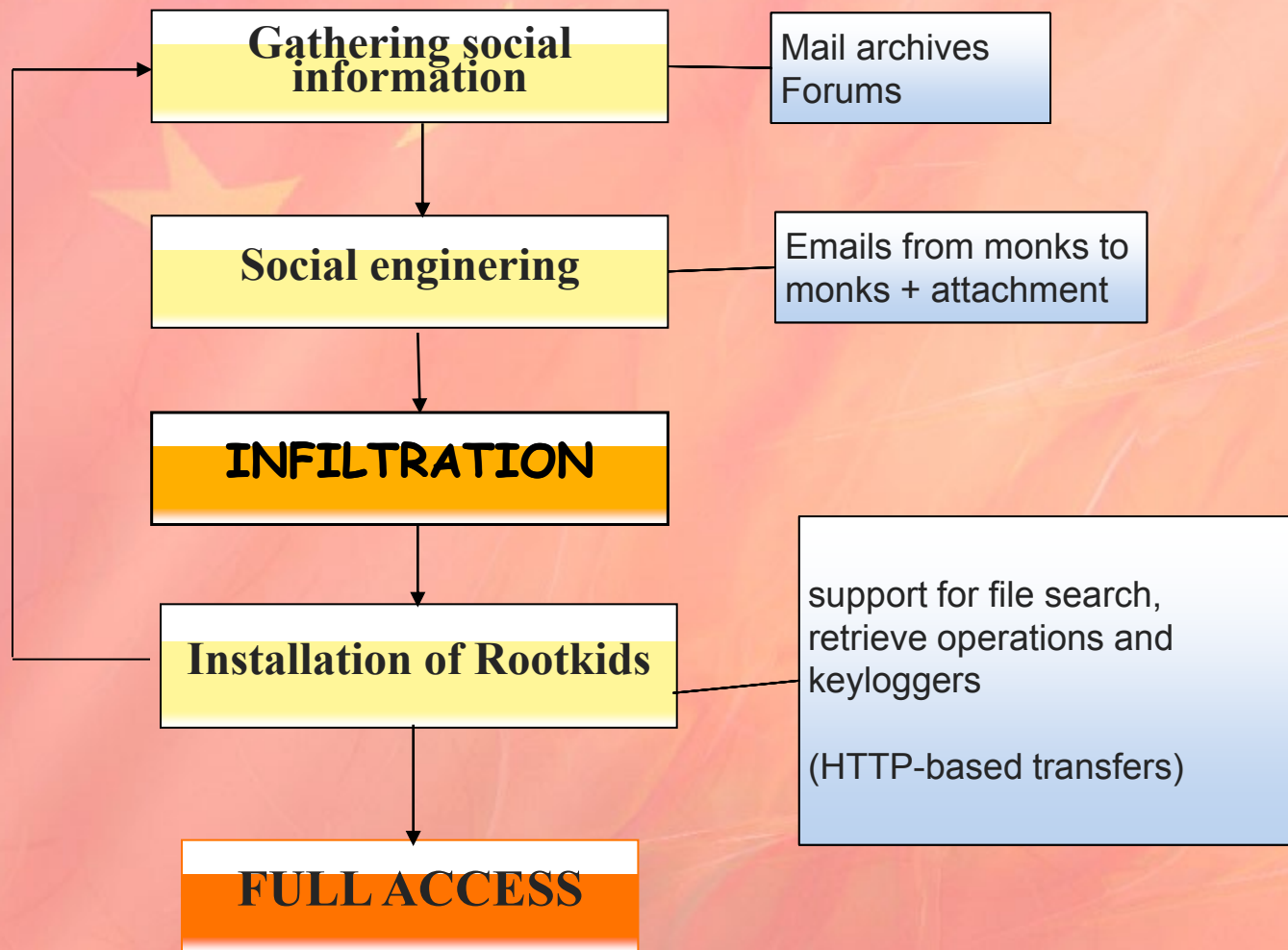
History

- Chinese invasion in 1950
- Uprising in 1959 - Dalai Lama escaped
- **OHHDL** (Office of His Holiness the Dalai Lama)
- Diplomatic and foreign meetings, Refugees
- IT (emails, web, forums, documents, DB)
- Secret contents

The attack

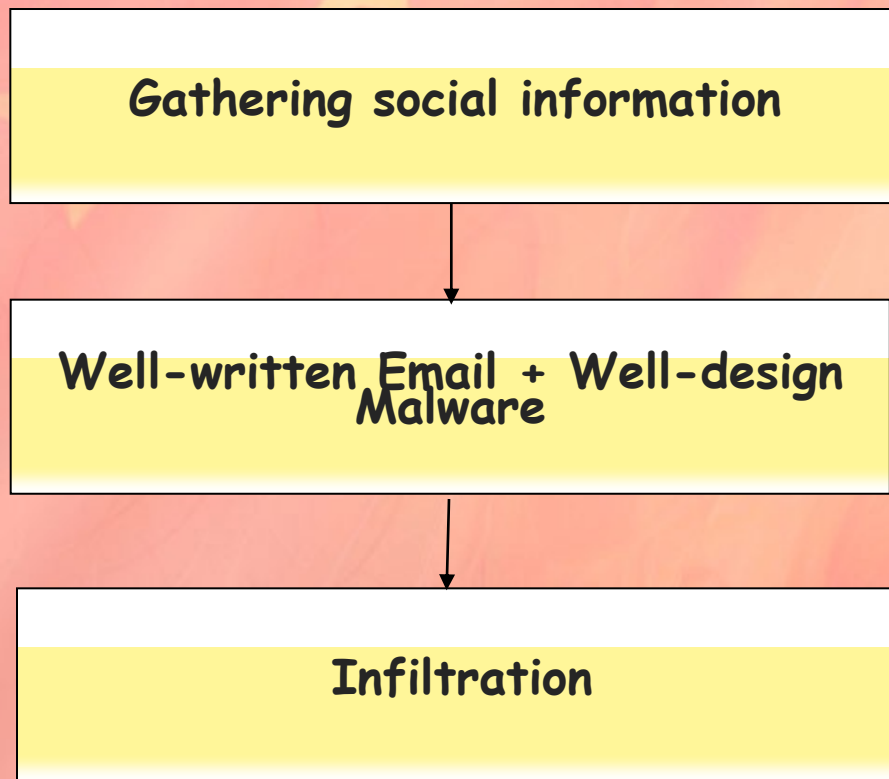
- Suspicion and Help from ONI-Asia
- Investigation:
 - connections to mail server from IPs in China and Hongkong)
 - suspicious file transfers
 - fraud emails with infected attachments

Assumptive Progression



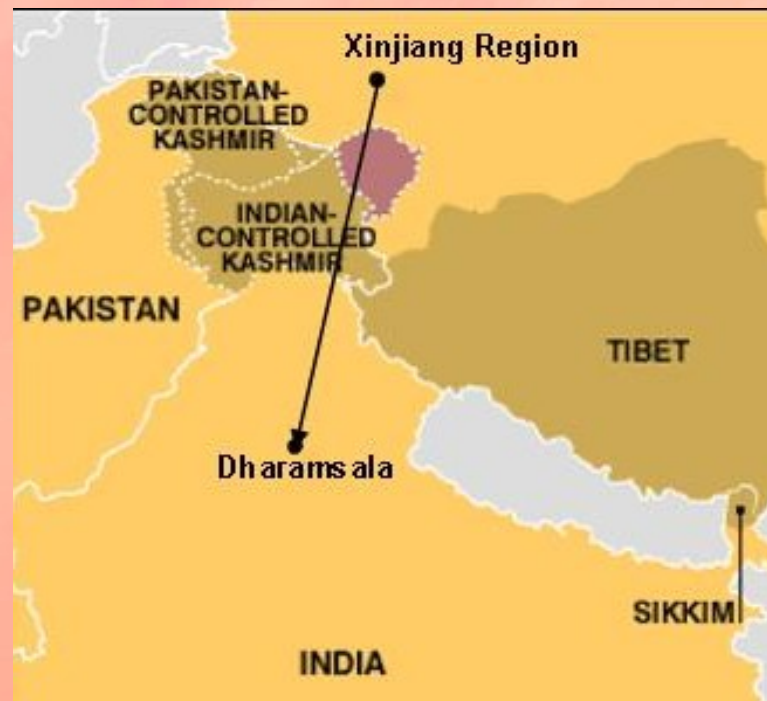
Social Malware

- From Social Phishing



Amaters!!!

- 1st mistake:
 - No operational security
 - No proxy, no anonymisers
 - Direct connections from Xinjiang Province
- 2nd mistake:
 - Exposure



Analysis

- The attack carried out by governmental entities but possibly by motivated individual
- Required skills:

Programing + Social Skills

Today good-quality malware available on the Internet:

Lamas or Llamas?

- Tibetan Security Model
 - users trusted will work sensibly
 - Sensitive files on local filesystem
 - No separation of sensitive and risky activities
- Capable Administrators

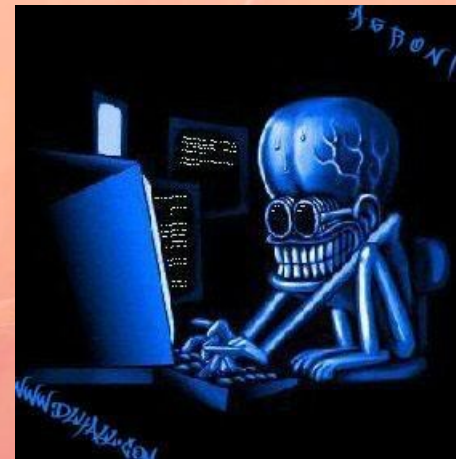



Countermeasures

- System of information clasification
- Use of systems with solid MAC support (SELinux, Trusted Solaris etc.)
- Operational security
- Red Team
- REALITY: expensive with high administrative cost. Many companies will not adopt.

Authors' Predictions

- Social response to the threat will be slow
- Users will be advised to work sensitively without exactly specifying how
- Avoiding Redresses 'wicked' contract terms
- Firms will not change their security models
- Hackers adopting social malware will have lovely times next few years.



The background features a warm gradient from light pink to orange, overlaid with a pattern of thin, white, wavy lines. In the upper left corner, there are several yellow, five-pointed stars of varying sizes, arranged in a diagonal line from the top left towards the center.

Thank you for your attention