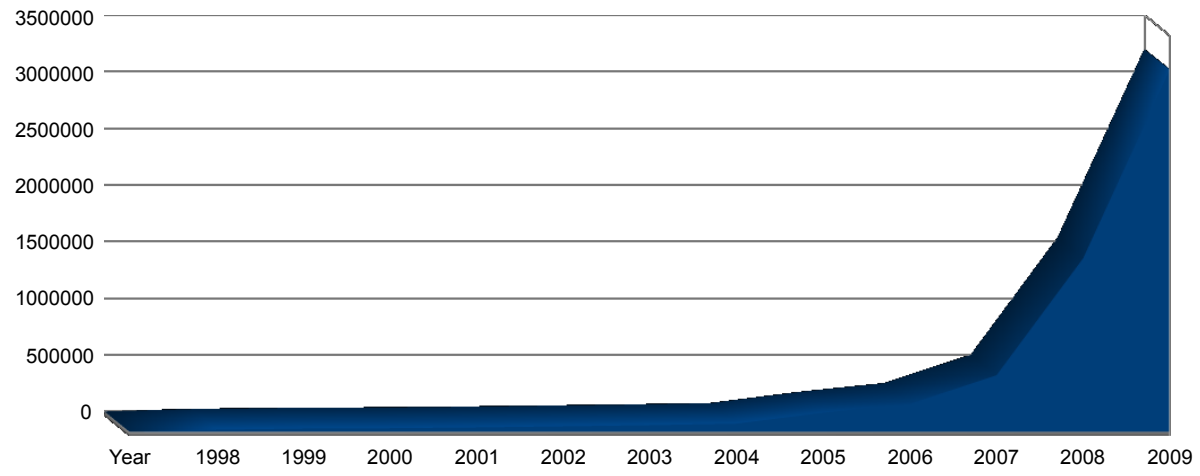

KASPERSKY lab
Back to the future:
Detecting the least polymorphic part
Roel Schouwenberg
Global Research & Analysis Team
CARO Workshop, Helsinki, Finland 2010

Overview

- Introduction
- The first problem and solution
- Alternative detection case studies
- Conclusions

Global stats

- ~40+k/day not seen before malware samples
- ~4.5M signatures per 21 May 2010



Problems (with 40k samples/day)

- Binaryitis
- Focus of detection and tests is binaries
- Samples lose relevance

- Tests focusing on large zoo sets
- Skewed results

- Working against innovation and real protection

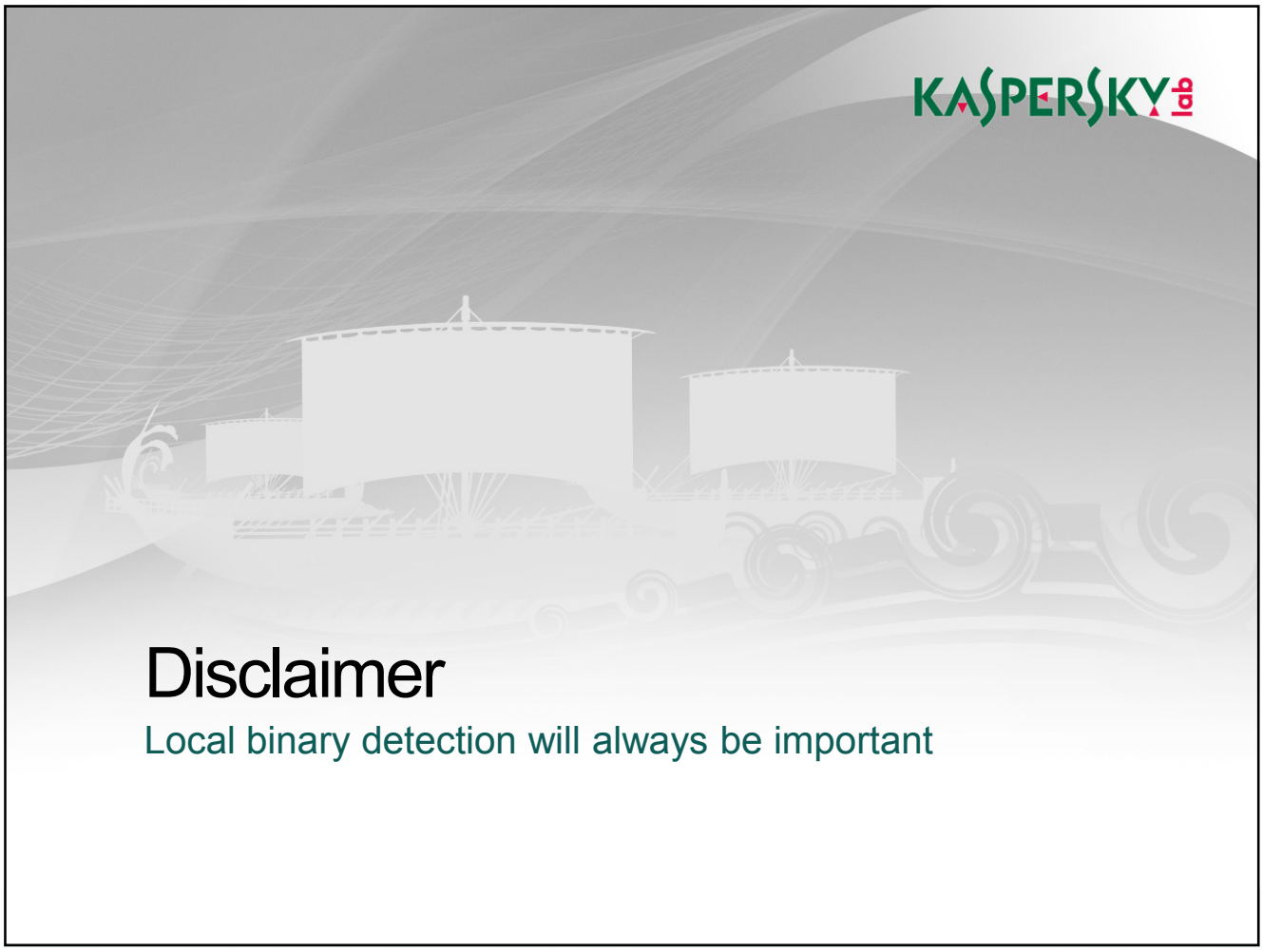
Solutions…

KASPERSKY lab

- And then there was AMTSO
- Whole product testing and whatnot
- Theoretically no more punishment for innovation

amtso

Anti-Malware Testing Standards Organization



Disclaimer

Local binary detection will always be important

Looking at the bigger picture

- Top prevalent threats
- Top complex threats
  - How's your data on TDSS infected machines? :-)
  - Utilize support as a resource
- Analyzing infection chain
- Front-end vs. back-end

Approaches

- Static binary/script detection
- Domain/URL detection
- Behavior detection
  - Registry, File and Network behavior

Koobface

- 10000s of binaries
- Served through the web via:
  hxxp://[domain]/.sys/index.html?getexe=fb.101.exe
  ….
  hxxp://[domain]/.sys/index.html?getexe=loader.exe
- Generic on hxxp://[domain]/.sys/index.html?getexe=
- No FPs, effective for more than half a year
- Use internal systems and search engine for checking
  – “inurl:”

Exploit packs

- Server-side polymorphic
- Pretty quick to react to generic script detection
  - hxxp://[domain]/ ld/dx
  - hxxp://[domain]/ld/eagle
  - hxxp://[domain]/cgi-bin/index.cgi?grey
  - hxxp://[domain]/load.php?id=???&spl=?
- Chances of FP are increasing
  - Still good for temporary detection till proper script detect

Fraudware – FakeAV

- Method of delivery social engineering or tech exploits
- Entire chain very polymorphic
- Detection on social engineering HTML and/or JS

- 01 2010:
  - #16 Trojan.JS.Fraud.s
- 03 2010:
  - #8 Trojan.HTML.Fraud.aj, #12 Trojan.HTML.Fraud.aq
- 04 2010:
  - #20 Trojan.HTML.Fraud.am

Qbot aka Qakbot

- Worm with backdoor functionality
  - Spreading strategy similar to Clampi
  - PSW stealer, Banker
- Same C&C used for (almost) half a year
- Detect on network connect

Detecting malicious web resources

- URL generics should have less FPs
- URL generics are far from perfect
  - Increased randomness may limit effectiveness
- Adobe Flash update generics
  - Total FP fest on clean set
  - Worked well on suspicious URL feed
  - Luckily, there are no web resources FP tests ;-)

What is a web FP?

KASPERSKY lab

- Site containing some malicious PE or script
  - With or without legitimate index
- To block or not to block the entire host/domain?
  - code.google.com ?
  - Smart automation needed
- Forcing webmasters to take action
- Testers will need our help

Conclusions

- Great opportunities for innovations
- Investigate family M.O.
- Determine which part of the chain gives best generic


KASPERSKY lab
Kiitos! Questions?
Roel Schouwenberg
Global Research & Analysis Team
CARO Workshop, Helsinki, Finland 2010