On the Evolution of Threats: Who is Faulty?

Marc Dacier

Director, Symantec Research Labs Europe

marc_dacier@symantec.com

LAAS-CNRS, Toulouse, 9/10/2008

Overview

- Introduction: 20 years ago, the Morris worm
  - High level overview of today's trends
  - IDSs, AVs, etc.
  - Assessing malicious fault detectors
- Conclusions

Morris Worm, aka Internet WORM

- 1988:
  - the Morris worm, aka Internet worm, spreads
  - During several days, entire branches of the Internet have been disconnected from the rest of the world
  - It created a shock and came as a surprise for many people.
- Was it really, totally, unexpected?

Historical background

- 1982:
  - “The ‘Worm’ Programs – Early Experience with a Distributed Computation”, J. Shoch and J. Hupp, Communications of the ACM, Vol. 25, N.3, March 1982, pp. 172-180.
    - Escaped in the Xerox Lab …
- Spring 1988:
  - The ADM Worm starts spreading in a stealthy way thanks to a buffer overflow vulnerability in DNS servers.
  - “ADM” stands for … “Association de Malfaisants” !

Historical background (ctd.)

- November 1988:
  - The Morris Worm, aka the Internet Worm
  - Complete analysis can be found in:
    - "An Analysis of the Internet Worm," Eugene Spafford, *Proc. European Software Engineering Conference*, pp. 446–468, Sep. 1989, *Lecture Notes in Computer Science #387*, Springer-Verlag.
  - The worm was targeting several *well known* vulnerabilities
  - It was not supposed to generate any harm
  - A « bug » caused it to overload machines and, hence, putting the Internet on its knees
- It boosted the deployment of firewalls, just invented a few years before by Bellovin and Cheswick.

More *historical* Worms

- July 19, 2001:
  - CRv2, aka Code Red I, *reuses* the same attack than another worm launched 6 days before.
  - Not for web site defacement anymore but *preprogrammed for DDoS* against whitehouse.gov
  - Stopped the same day at midnight UTC, started again on Aug. 1st
  - Had contaminated almost all vulnerable platforms before halt.
- August 4, 2001:
  - Code Red II, different codebase than Code Red I, but similar targets.
  - Installs a rootkit, *opens a backdoor* in compromised system.
  - Uses a *better propagation strategy*
- September 18, 2001:
  - Nimda strikes with *5 different attack techniques* bundled in a single worm.
  - Spreads very quickly and offers full control to remote master.

Expectations for/in 2001 …

- According to Staniford, Paxson and Weaver [SPW01], the next generation of worms could hit the whole Internet in less than 30 seconds!
  - "[…] In conclusion, we argue that a compact worm that begins with a list including all likely vulnerable addresses, and that has initial knowledge of some vulnerable sites with high-bandwidth links, appears *able to infect almost all vulnerable servers on the Internet in less than thirty seconds*."
- They realised later that they were wrong: less than 5 seconds would be enough.
- They are right but, fortunately, it did not happen … yet.

Overview

- Introduction: 20 years ago, the Morris worm
  - High level overview of today's trends
  - IDSs, AVs, etc.
  - Assessing malicious fault detectors
- Conclusions

Internet Security Threat Report XIII Important Facts

Data Sources

- Symantec Global Intelligence Network
  - 40,000 registered sensors in 180 countries.
  - 120 million desktop, gateway and server antivirus installations.
  - 25,000 vulnerabilities in the Symantec vulnerability database.
  - 2,000,000 decoy accounts in the Symantec Probe Network - 30% of all email traffic
- Symantec Global Coverage
  - 4 Security Operations Centers, 11 Symantec Research Centers.
  - Symantec software protects more than 370 million computers or email accounts worldwide, and 99% of the Fortune 1000 utilize Symantec products.

What the ISTR is:

- A detailed report on trends that ***Symantec*** sees.
- Based on real, ***empirical*** data collected by the Global Intelligence Network.
- Only publicly available report to offer a ***complete*** view of the current Internet security landscape.
- Identifies and ***analyzes*** attacker methods and preferences.
- Vendor ***neutral.***

What the ISTR is not:

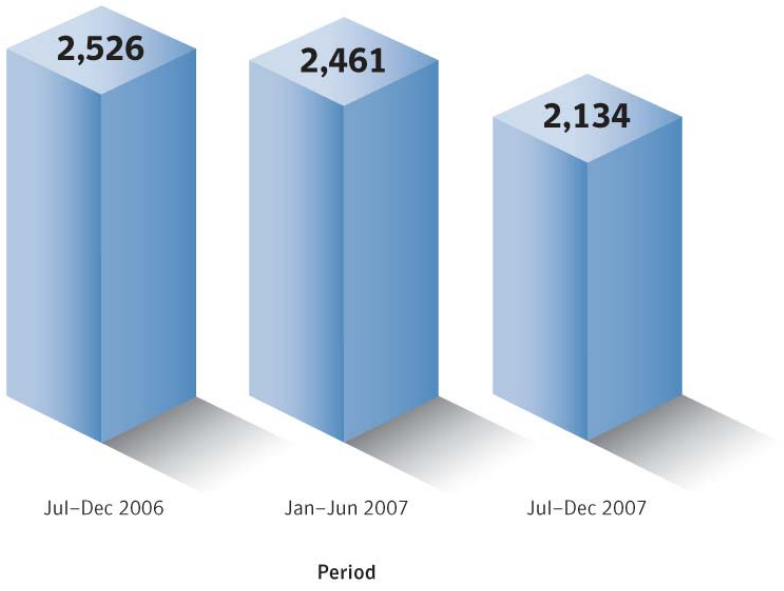
- A ***survey*** of opinions.
- Product driven ***marketing.***
- Scientific ***certainty.***

Threat Landscape – Overarching Themes

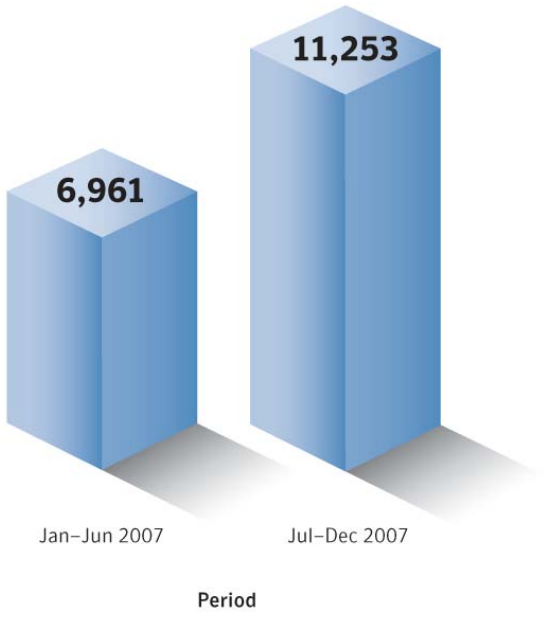
- The Web is quickly becoming the distribution point for malicious code and attacks
- Malicious activity that targets end-users rather than computers
- Consolidation and maturation in the Underground Economy
  - Specialized production and provisioning
  - Outsourcing
  - Multivariate pricing
  - Flexible business models
- Rapid adaptability of attackers and attack activity

The Web as the Focal Point

- Vulnerabilities in websites are more popular because they allow for more sophisticated and multi-staged attacks.
- Site-specific vulnerabilities outnumber traditional vulnerabilities nearly 5 to 1 with much lower patch rates – only 473 of the site-specific vulnerabilities had been patched at the time of reporting.



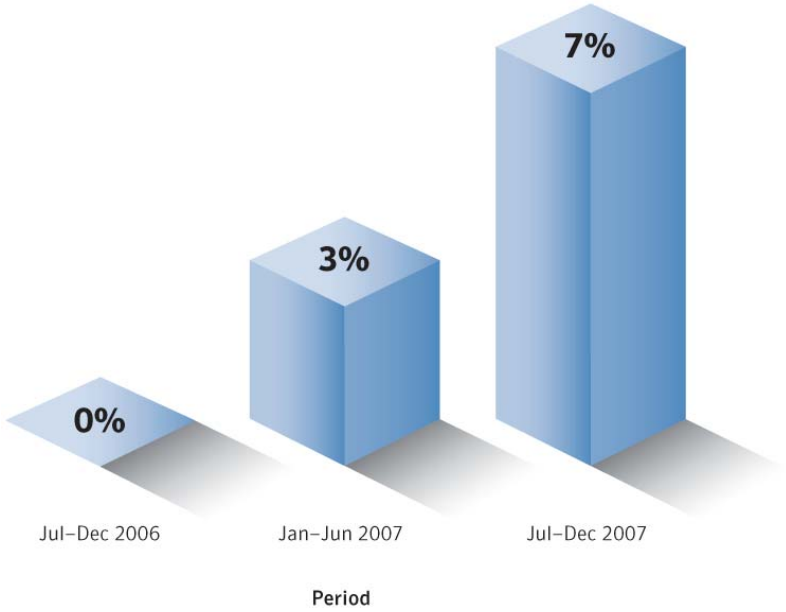
Vulnerabilities - Traditional



Site-specific vulnerabilities

Malicious Code Trends
Malicious code that modifies Web pages

- 7% of the top 50 malicious code samples modified Web pages on computers they compromise
- Two of the top ten new malicious code families modify Web pages
- Increase may be due to success of kits like MPack.

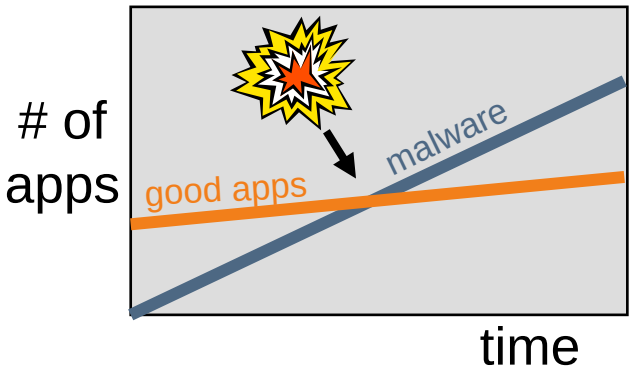


Bad vs. Good detectors

- **Traditional approach to malware detection and prevention is blacklist driven**
  - Find something bad
  - Write a virus signature
  - Deploy to the field

⇦ This year, we're on target to write > 1M new virus signatures!

- **However as each year goes by it becomes harder and harder to keep up…**
  - We are fast approaching an inflection point
  - Soon more malicious programs will be created than legitimate applications each year
- **Conclusion**
  - A new approach is needed!

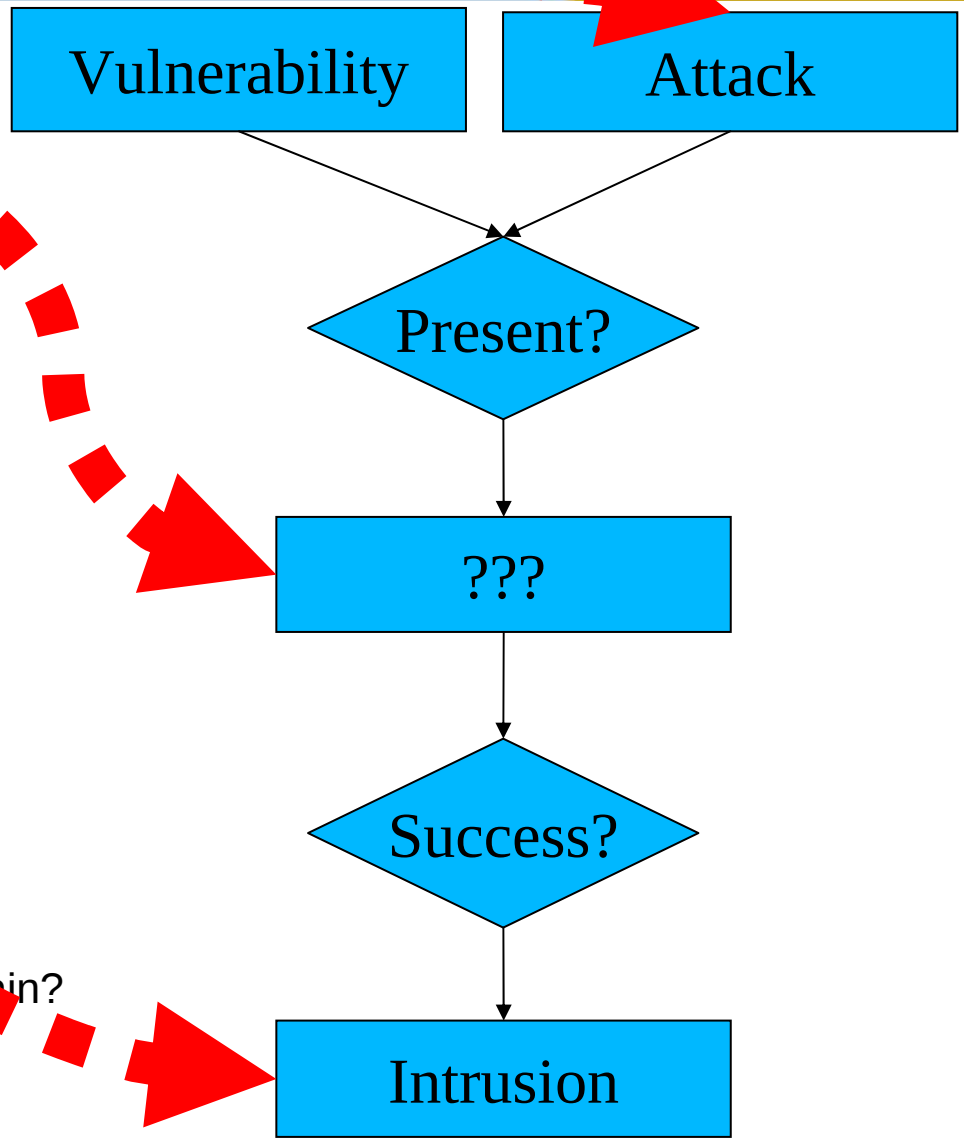


Overview

- Introduction: 20 years ago, the Morris worm
  - High level overview of today's trends
  - IDSs, AVs, etc.
  - Assessing malicious fault detectors
- Conclusions

Fault Tolerance

- Error Proc[illegible]g:
  - Intrus[illegible]tection
    - Is som[illegible]oing wrong?
  - Error diagnosis
    - What is really going wrong?
  - Error Recovery
    - How can I fix the situation?
- Fault Treatment:
  - Attack Attribution
    - What is the cause of this error?
  - Fault Passivation
    - Can I prevent it from happening again?



Paradigms

- Behaviour based (paranoiac)
  - If you do not recognize, it is suspicious

- Knowledge based
  - If you do recognize, it is suspicious

- ***Question: which one is best ?***

Overview

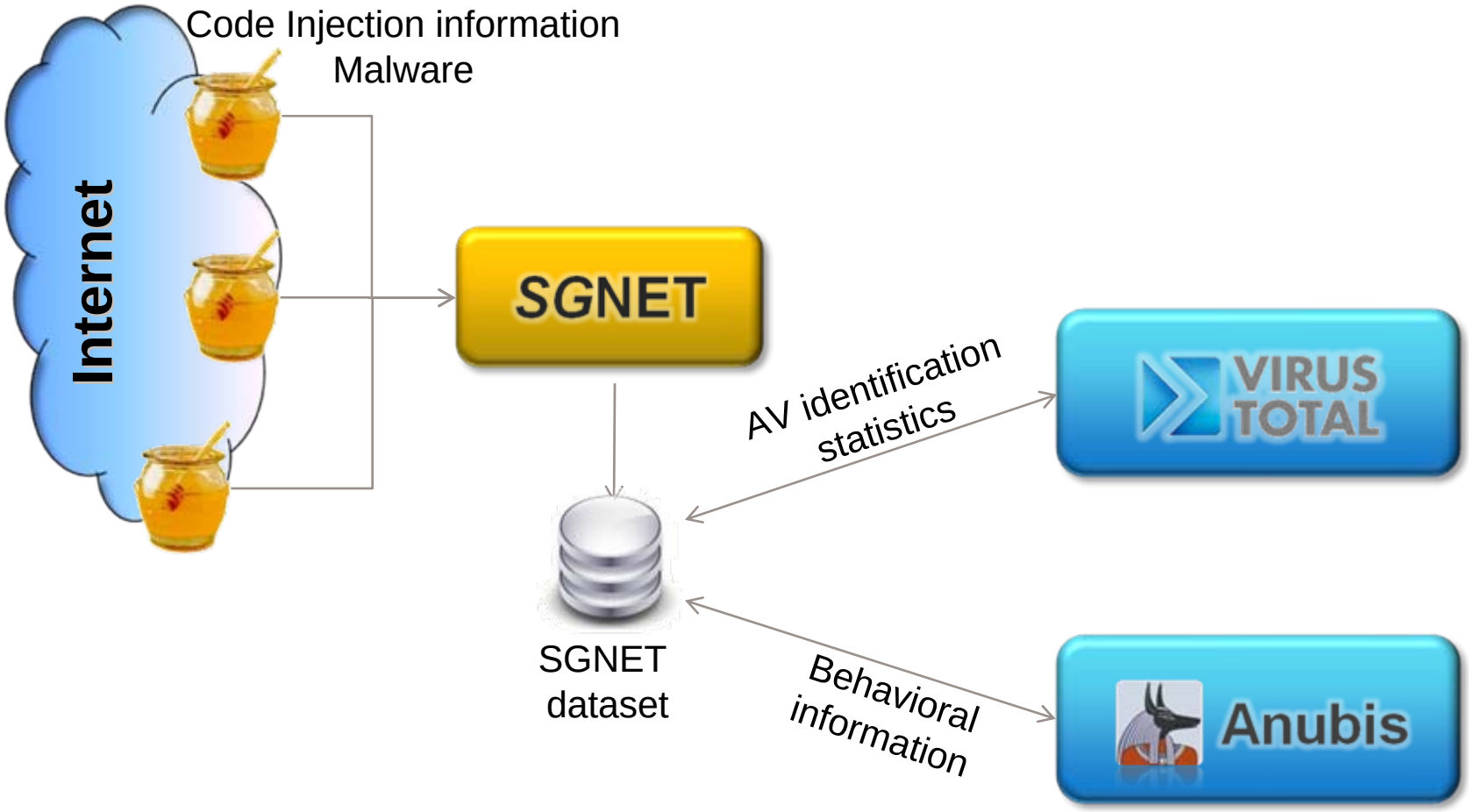
- Introduction: 20 years ago, the Morris worm
  - High level overview of today's trends
  - IDSs, AVs, etc.
  - Assessing malicious fault detectors
- Conclusions

WOMBAT Project

- The results presented here after come from the work currently carried out within WOMBAT, a EU funded project in the Seventh Framework Programme of European Research (FP7)
  - http://www.wombat-project.eu/

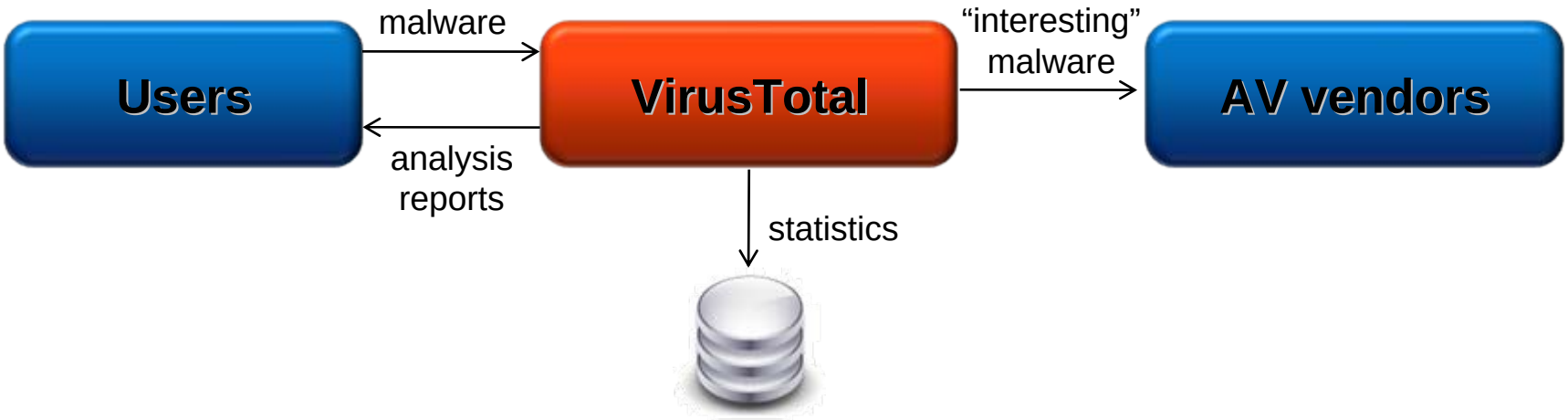
- **Academics:** TU Vienna, VU Amsterdam, Politecnico di Milano
- **Research Institutes:** EURECOM, FORTH, Institute for Infocomm Research - Singapore
- **CERTs:** NASK
- **Industrial partners:** France Telecom, Symantec

Our framework



VirusTotal

- Developed and maintained by Hispasec Sistemas
- Freely accessible via a web interface
  - www.virustotal.com
  - Support for 36 AV engines (command line interface only)
  - Widely known and used by the security and AV community



Anubis

- Automated analysis of an executable file by understanding its actions
  - Modifications to Windows registry
  - Modifications to filesystem
  - Interactions with the Windows Service Manager
  - Generated network traffic
- Web interface freely accessible to submit malware and retrieve the detailed report
  - http://anubis.iseclab.org

Submission policies

- Whenever a sample is collected by SGNET, how to relate it to the information provided by Anubis/VirusTotal?
- Anubis
  - Every sample is submitted only once
- VirusTotal
  - How does the detection performance evolve with time?
  - Daily submissions
    - At least 30 days
    - Stop after 7 identical reports

Research Challenges

- Interesting challenges derived from our experience with the SGNET dataset

Challenge 1

- Proliferation of different malware variants
- How to define a set of samples representative of the current malware scenario at any point in time?

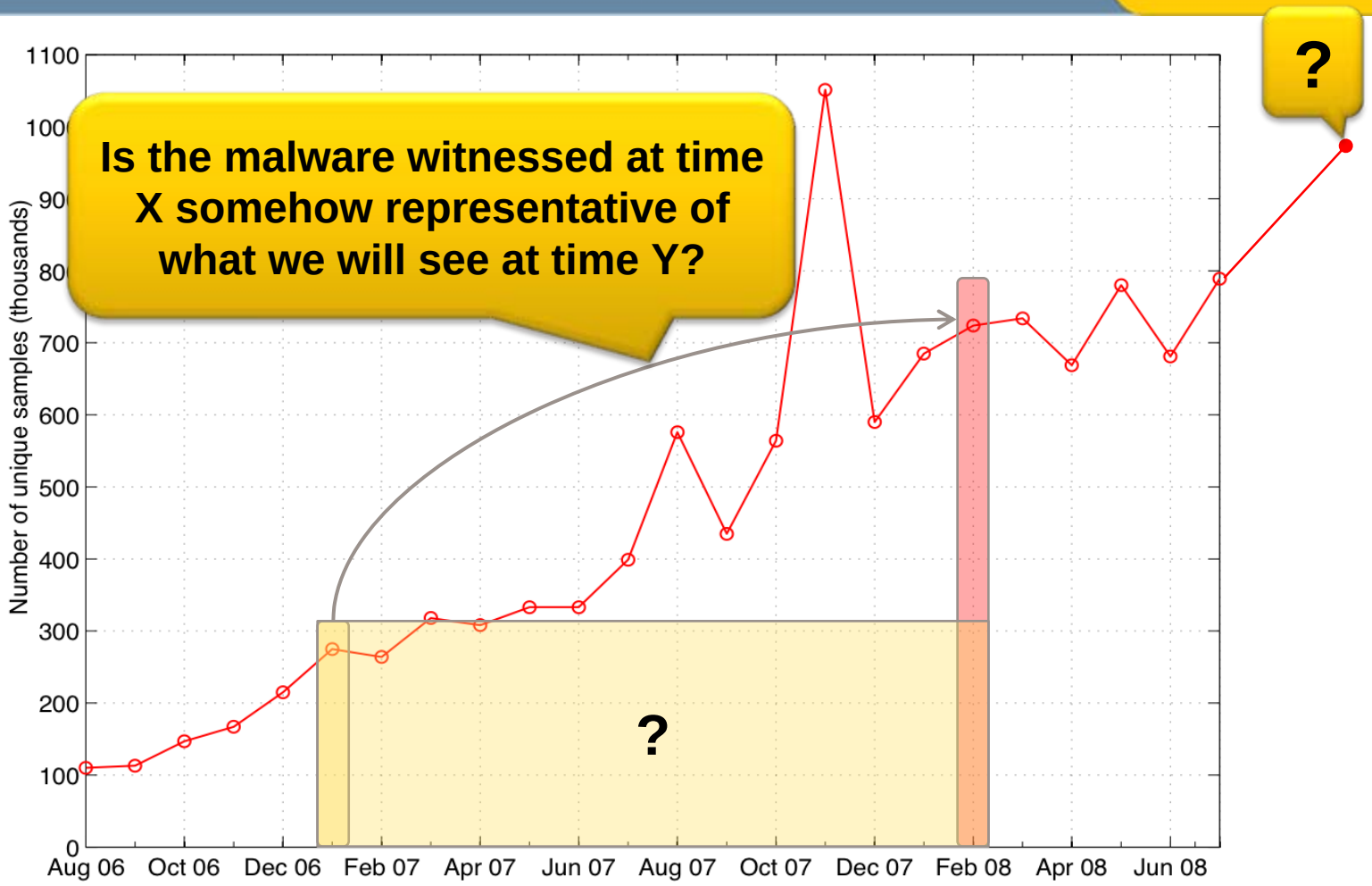
Challenge 2

- Does the absence of an expected detection always imply a failure of the detector?

Challenge 3

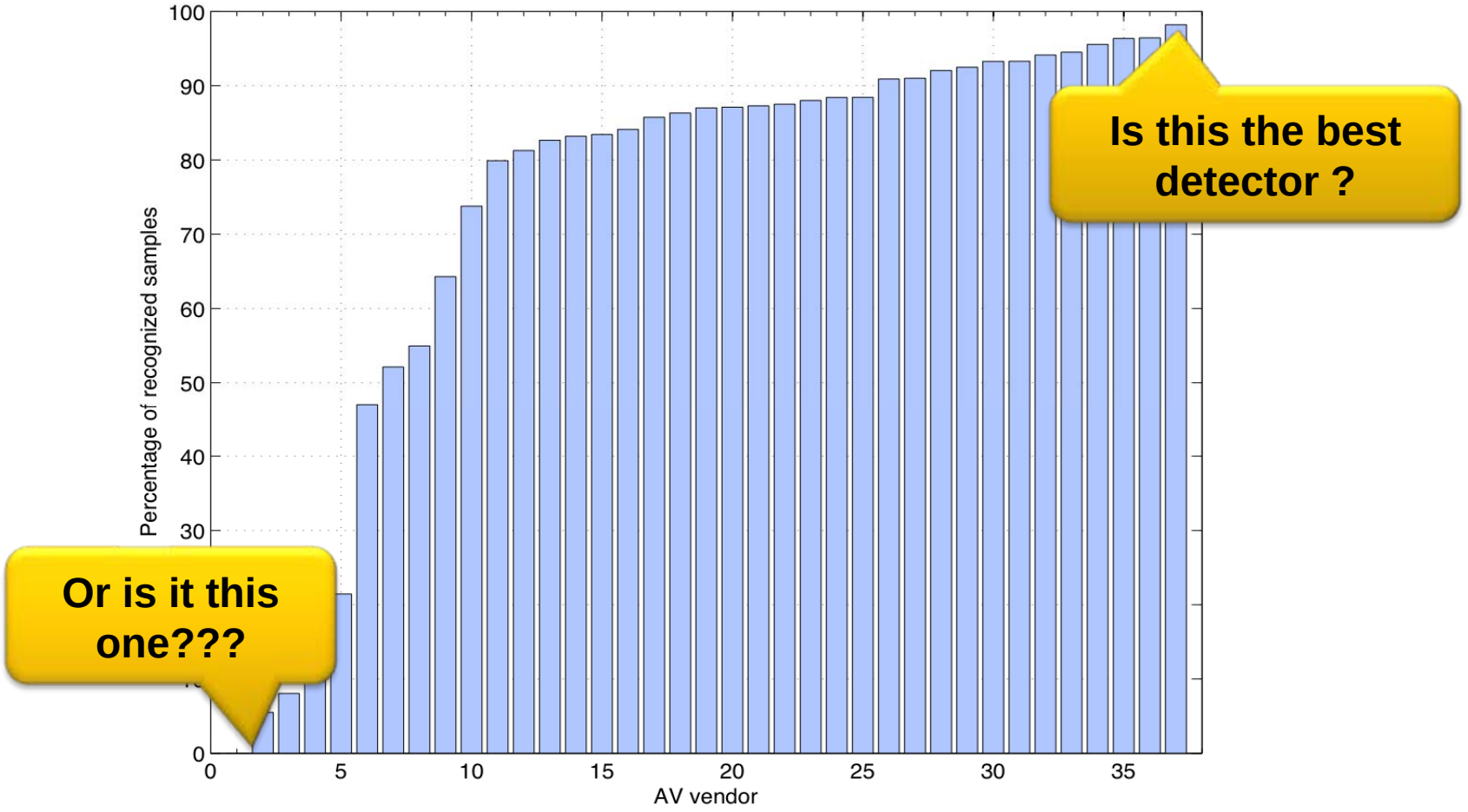
- Does the presence of an expected detection a sufficient condition to guarantee the absence of failure of the detector?

Challenge 1
Will we eventually succeed in …?



Distinct samples observed by the VirusTotal service every month

Challenge 2
Is an unraised alert always a false negative?



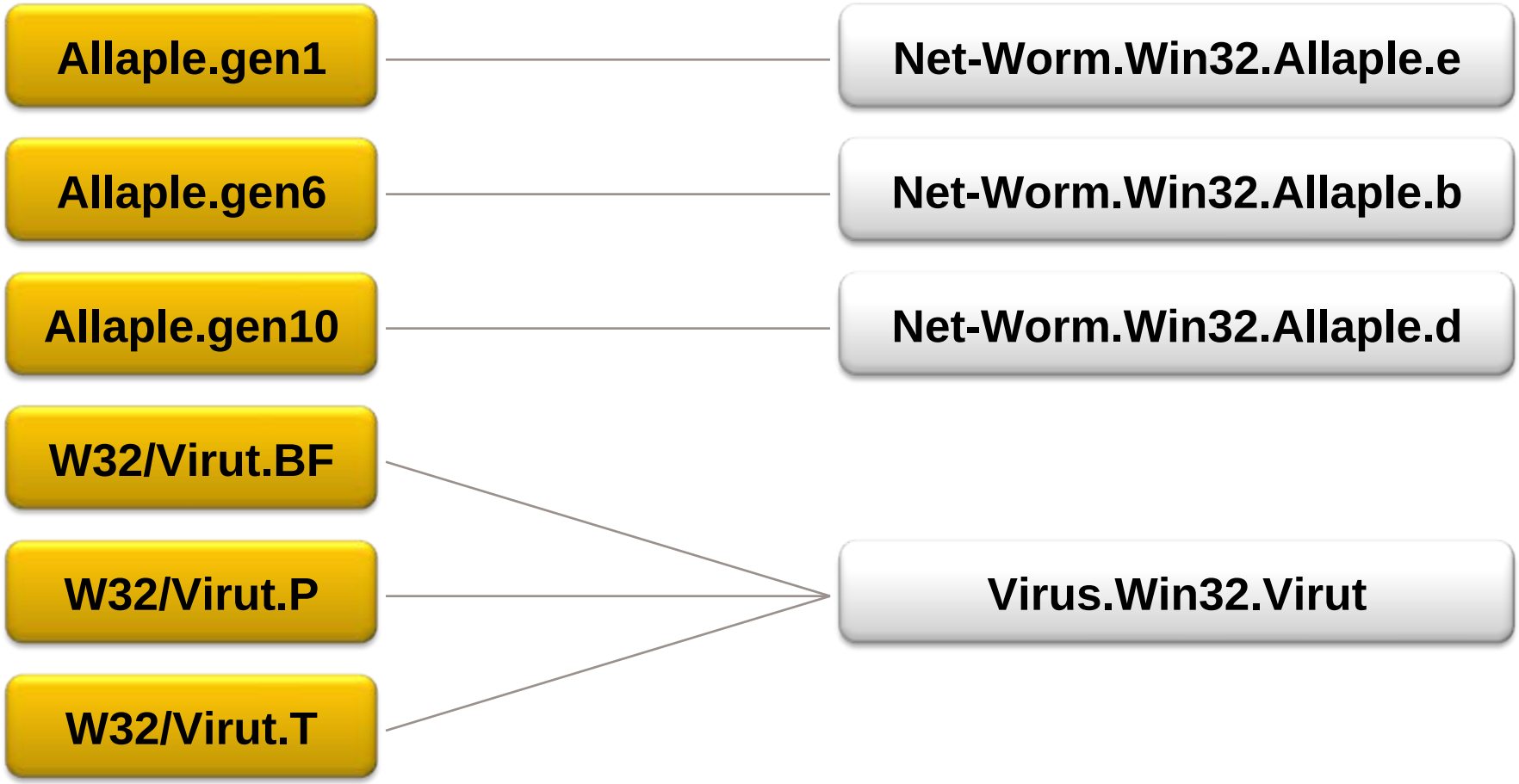
Percentage of samples detected by the different AV vendors for a selected class of samples in our dataset

Challenge 3
Can a valid raised alert be a false positive?

- If an alert has to be raised and indeed has been raised, is it a true positive?
  - If an alert A has to be raised and an alert B has been raised, is it a true positive?
  - How do you know A has to be raised in the first place?

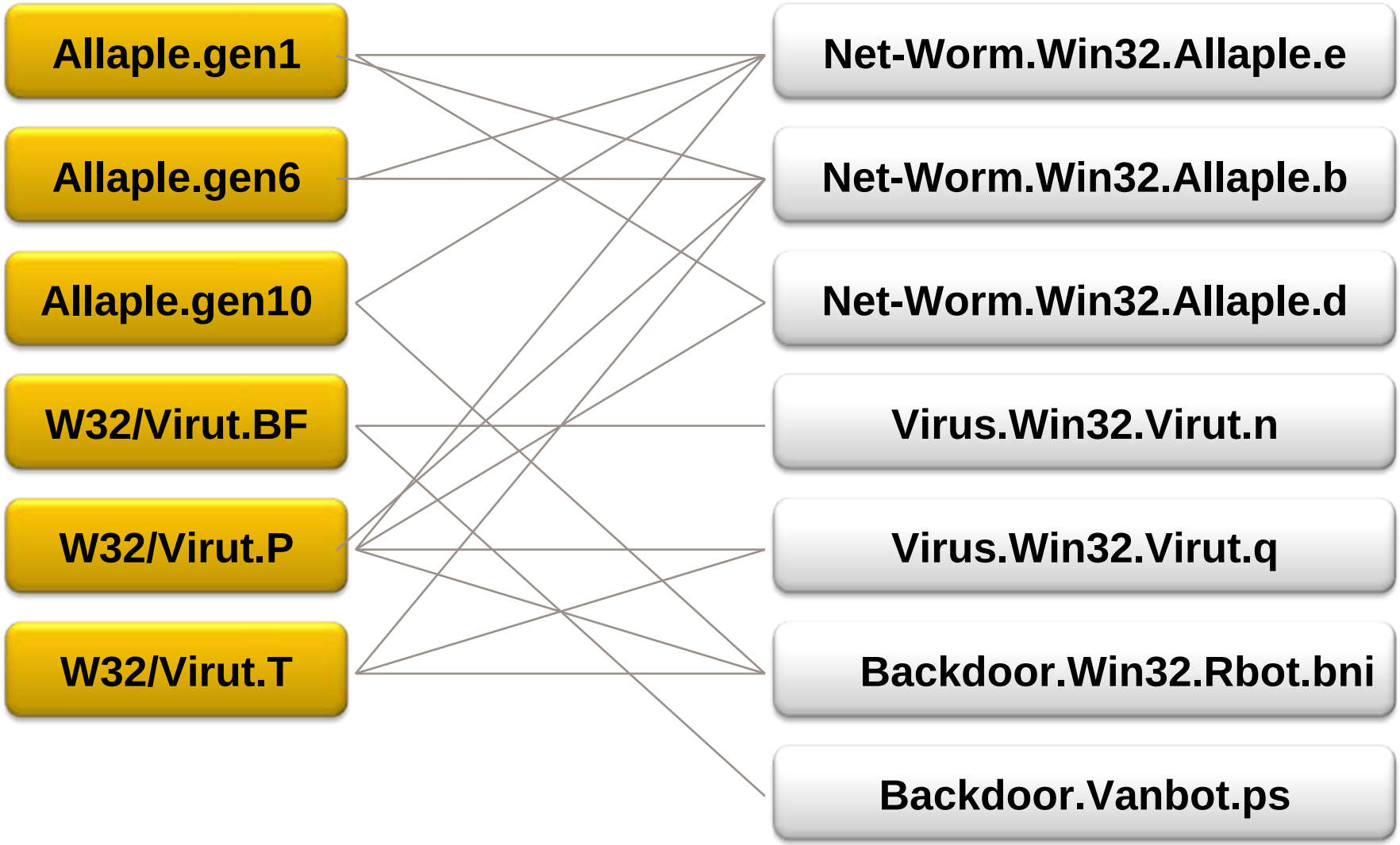
- In our dataset, 10314 modifications were detected in the label associated by a vendor to a given sample over the submission period (1081 unique types of modifications)
  - Example:

Labeling
What we would expect…



1:n relationships are allowed: for instance, one vendor uses a more generic label than the other

Labeling
… and what we get in practice



Overview

- Introduction: 20 years ago, the Morris worm
  - High level overview of today's trends
  - IDSs, AVs, etc.
  - Assessing malicious fault detectors
- Conclusions

Conclusion

- Threats are changing, rapidly
- There is a need to continuously verify the validity of the fault assumptions our detectors are based upon.
- Assessing the “quality” of the detectors is a challenging task because:
  - The mere existence of a “good testing dataset” is questionable.
  - Without precisely knowing what we want to do, we cannot define unambiguously the concepts of False Positive and False negative.
- But we need much more: what we really want is to assess the probability of failures, taking countermeasures into consideration as well !!!

Thank You!

Marc Dacier

marc_dacier@symantec.com