Security in knowledge

Lessons learned from a rigorous analysis of two years of zero-day attacks

Symantec Research Labs

Marc Dacier, Leylya Yumer, Tudor Dumitras

Session ID: HT-R07

Session Classification: Intermediate

Symantec.

RSA CONFERENCE EUROPE 2013

Take away messages

- This seminal work shows that 0-day attacks are not a new phenomena. Old data reveal their hidden existences
- Big data analysis is key to deal with today's threats.
- Therefore, data sharing is more important than ever.
- We offer the WINE environment to external researchers to foster scientific and rigorous experiments with representative real world data.

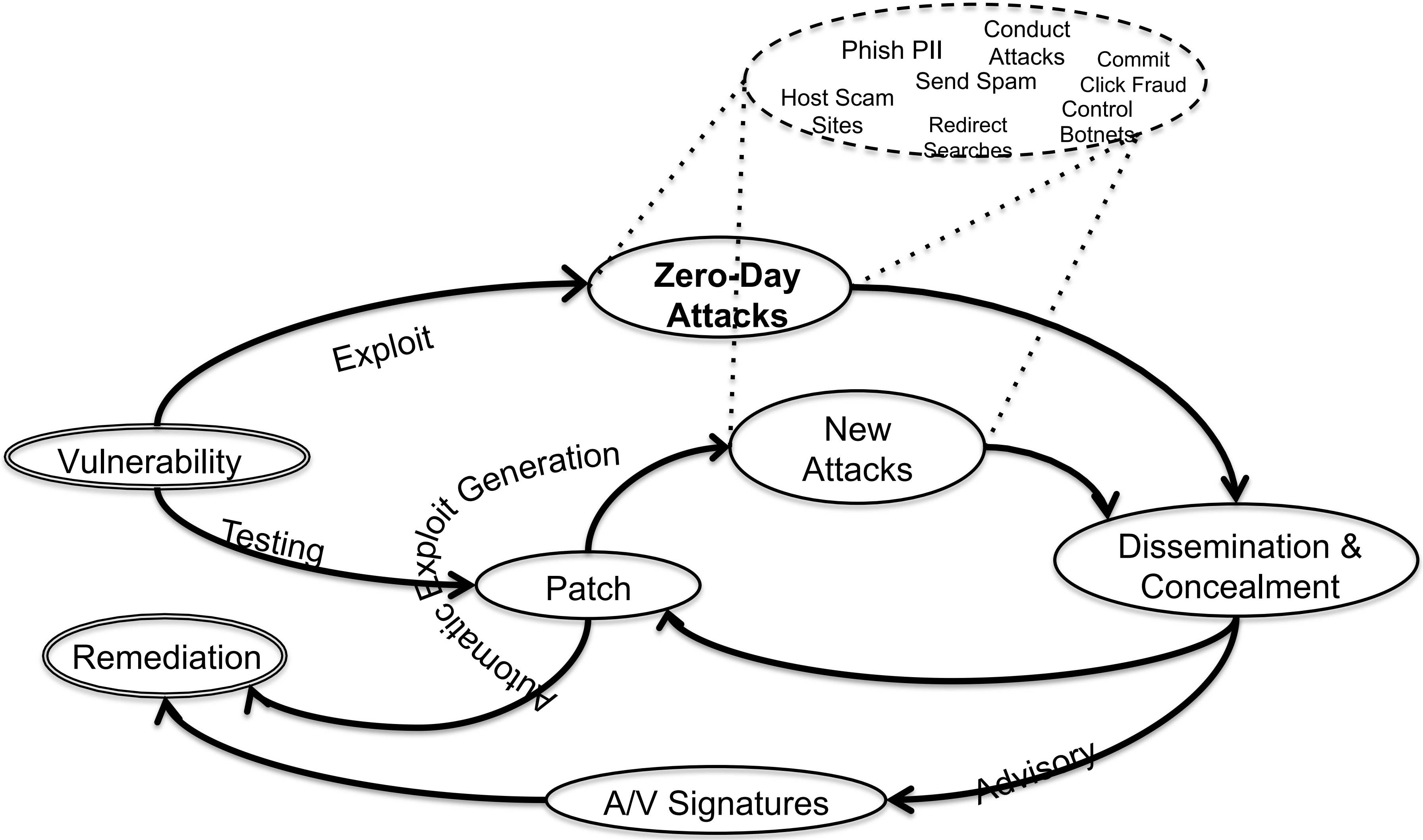
0-Day attack: Definition

- Takes advantage of unknown vulnerabilities on programs before
  - Are discovered
  - Are publicly disclosed
  - Have a security patch provided by the software vendor

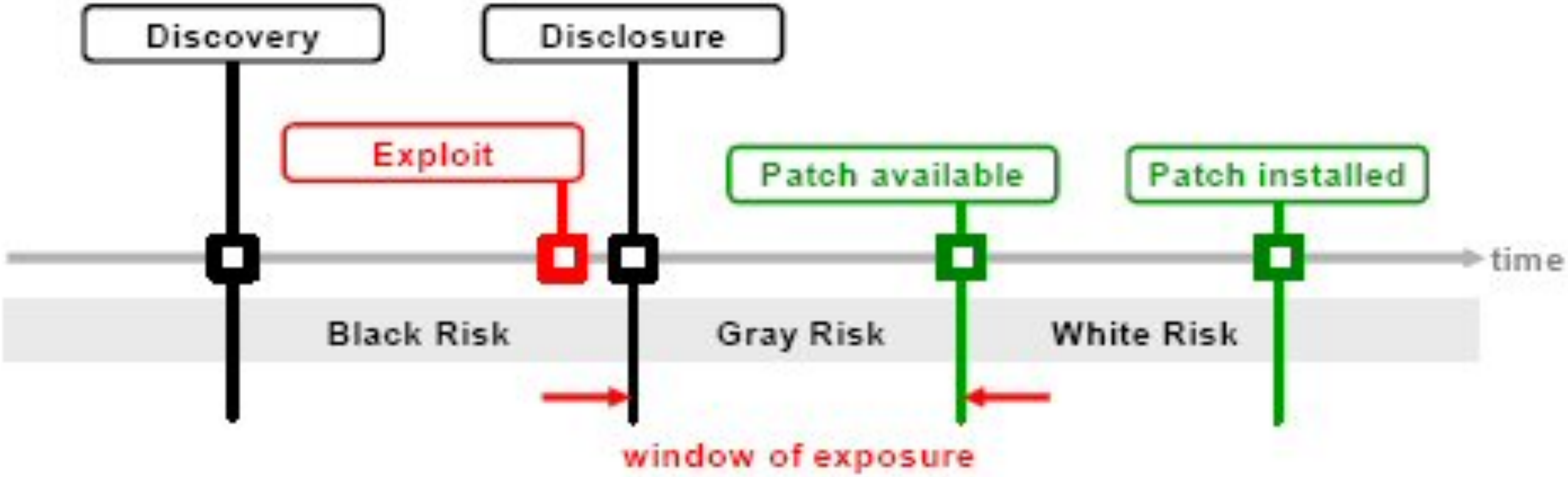
- Common definition
  - An attack that uses a zero-day (0-day) exploit

- Generic definition
  - An attack that compromises computers with unknown methods

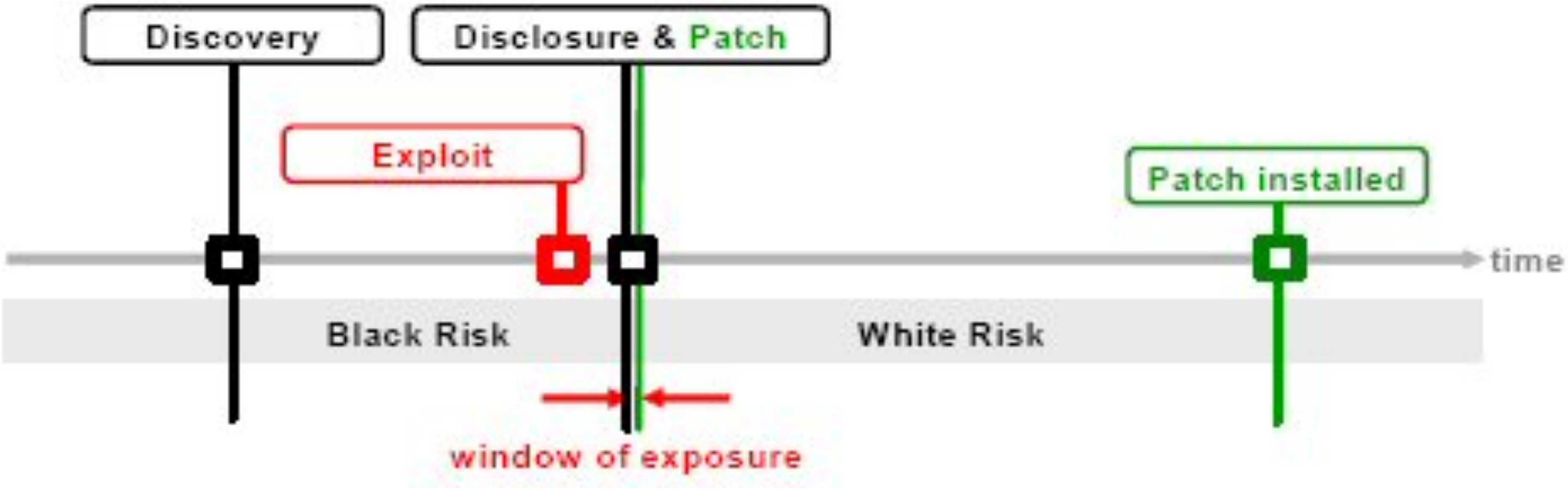
Vulnerability lifecycle



Life-cycle of a vulnerability

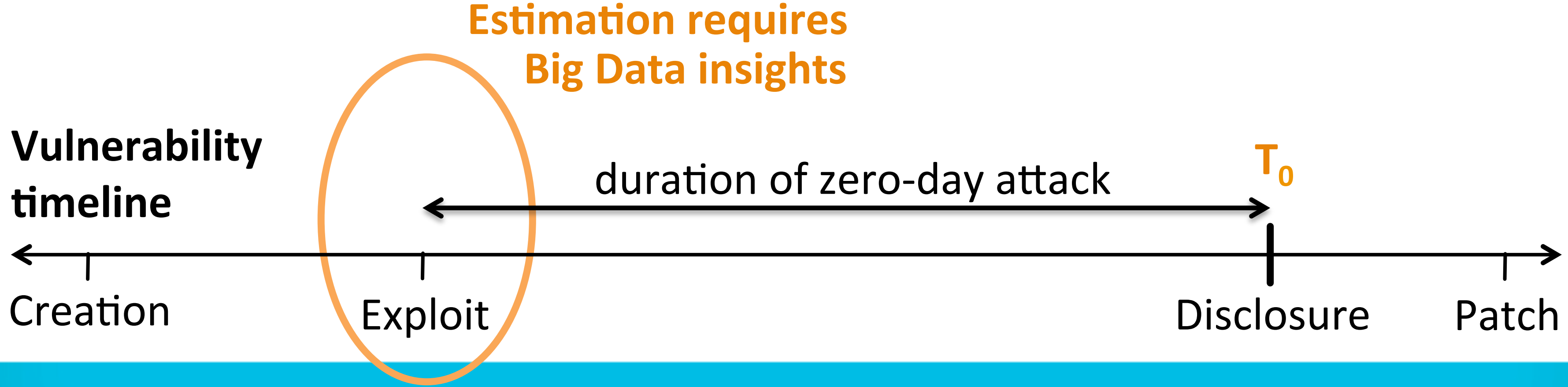


Life-cycle of a vulnerability



Research Questions

- **Are there more** zero-day vulnerabilities in the wild that we are not aware of?
- What is the typical **duration of zero-day attacks**?
- What is the **prevalence** of zero-day attacks?



Building the ground-truth?

- Since 1996, some sources provide information about known vulnerabilities
  - IBM-ISS, SecurityFocus, Secunia, CERT, SecurityTracker, SecWatch, FrSirt

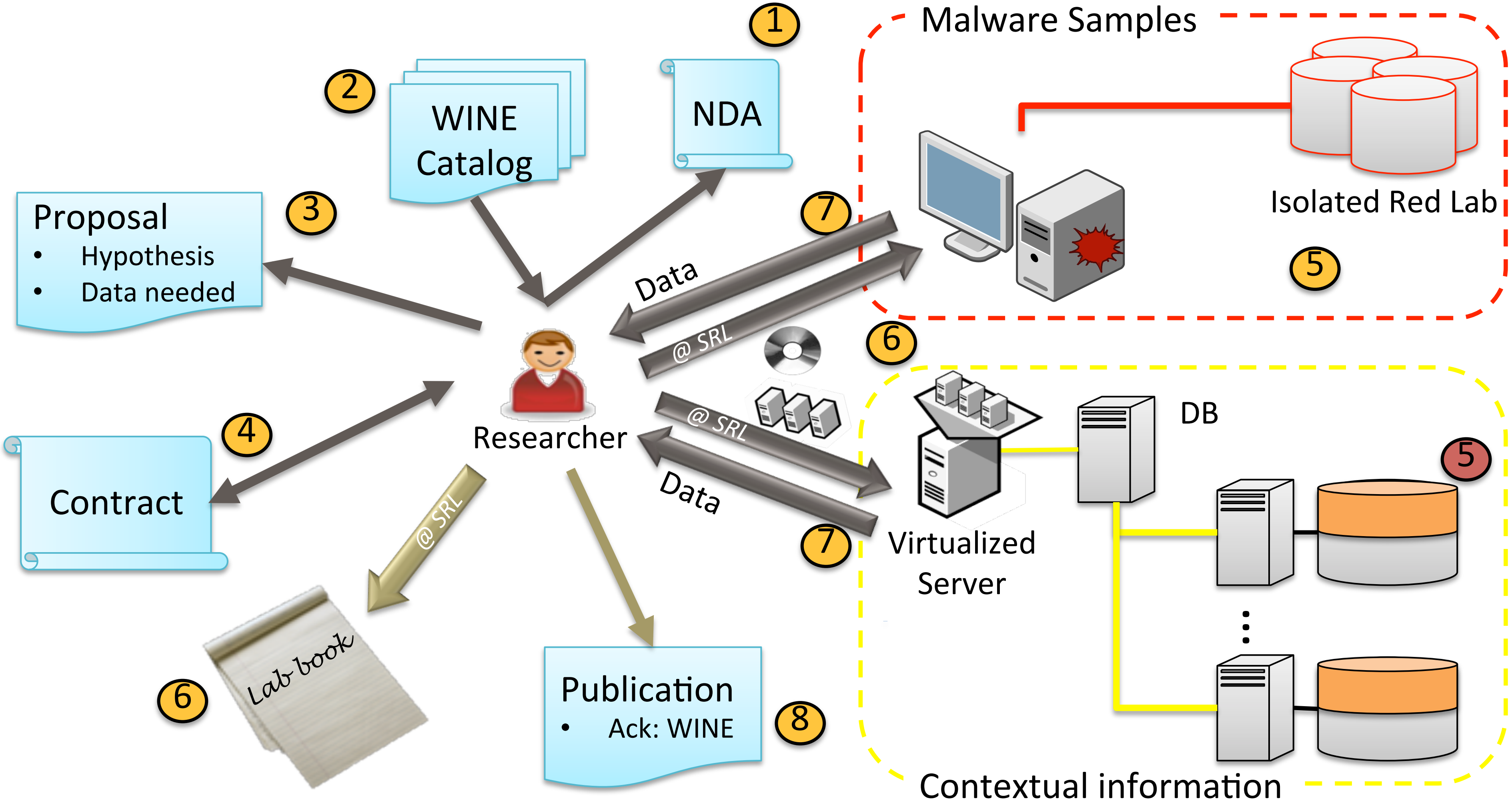
- Databases that correlate the information
  - National Vulnerability Database (NVD)
  - Open-source Vulnerability Database (OSVDB)

- A standardized identifier for known vulnerabilities
  - Common Vulnerabilities and Exposures (CVE)

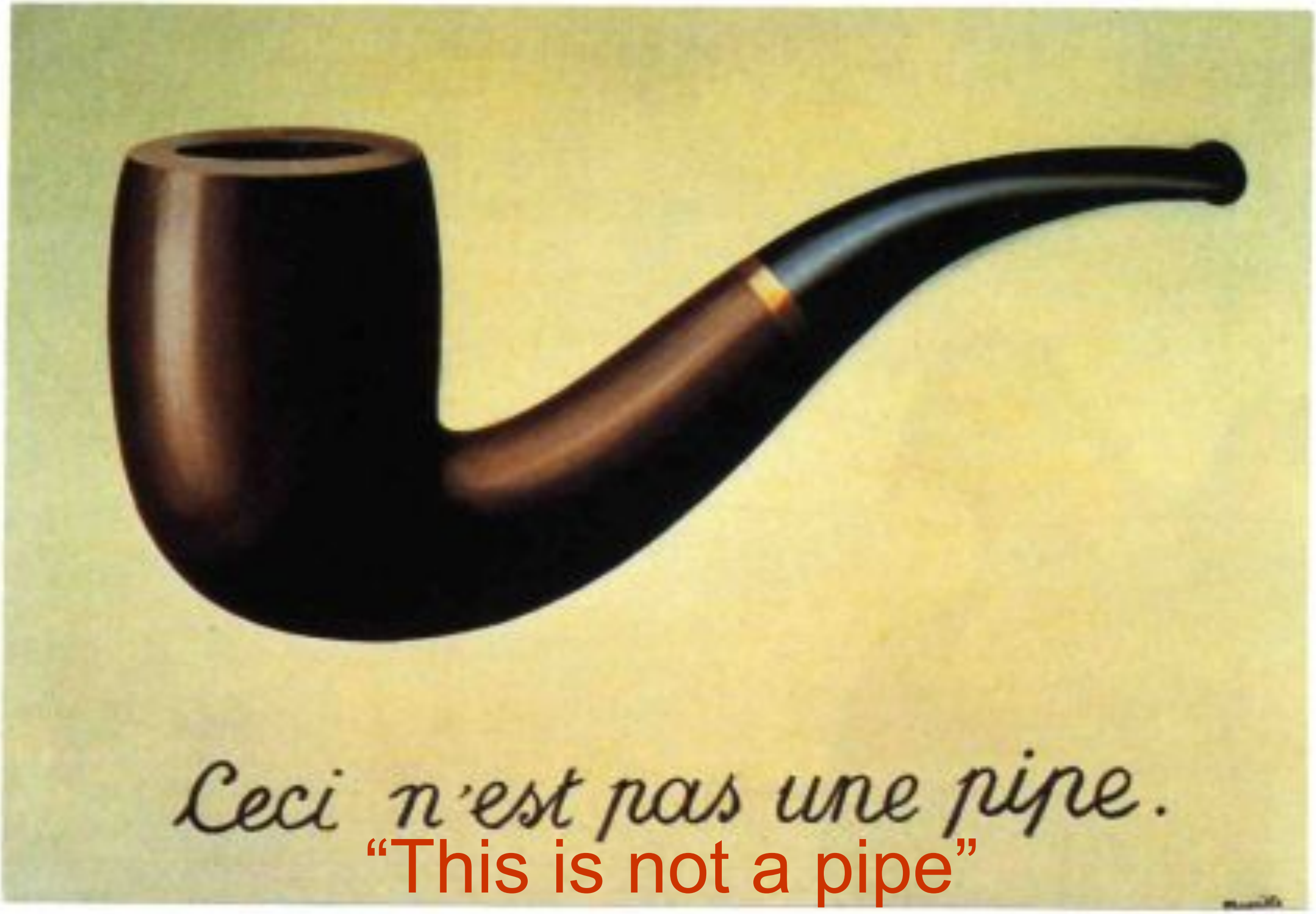
WINE

- The Worldwide Intelligence Network Environment (WINE)
  - Malware Samples
  - Binary Reputation
  - A/V Telemetry
  - URL Reputation
  - Email Spam
  - IPS Telemetry
  - DNS Data

WINE: Operational Model



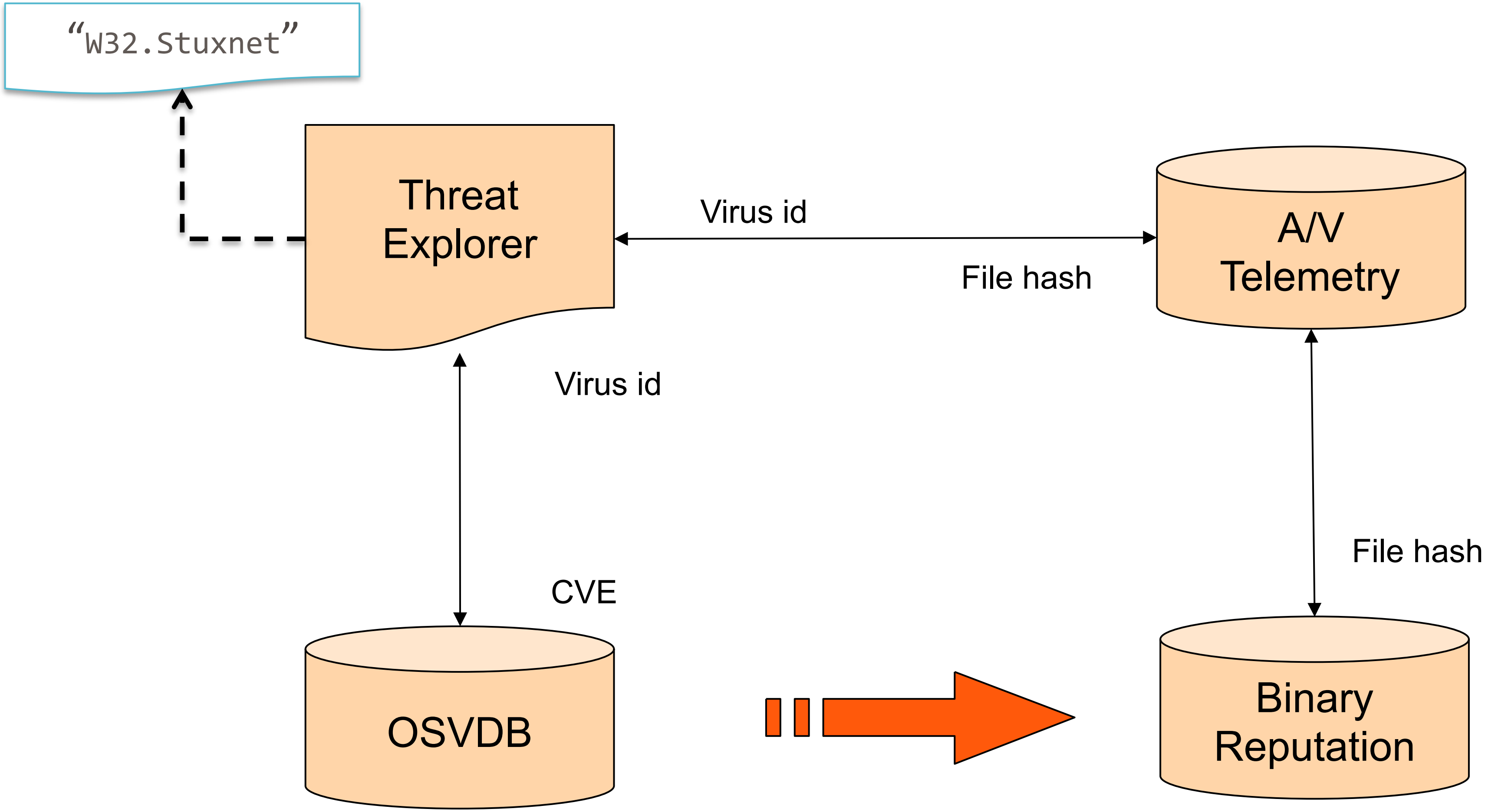
Beware



“This is not a pipe”

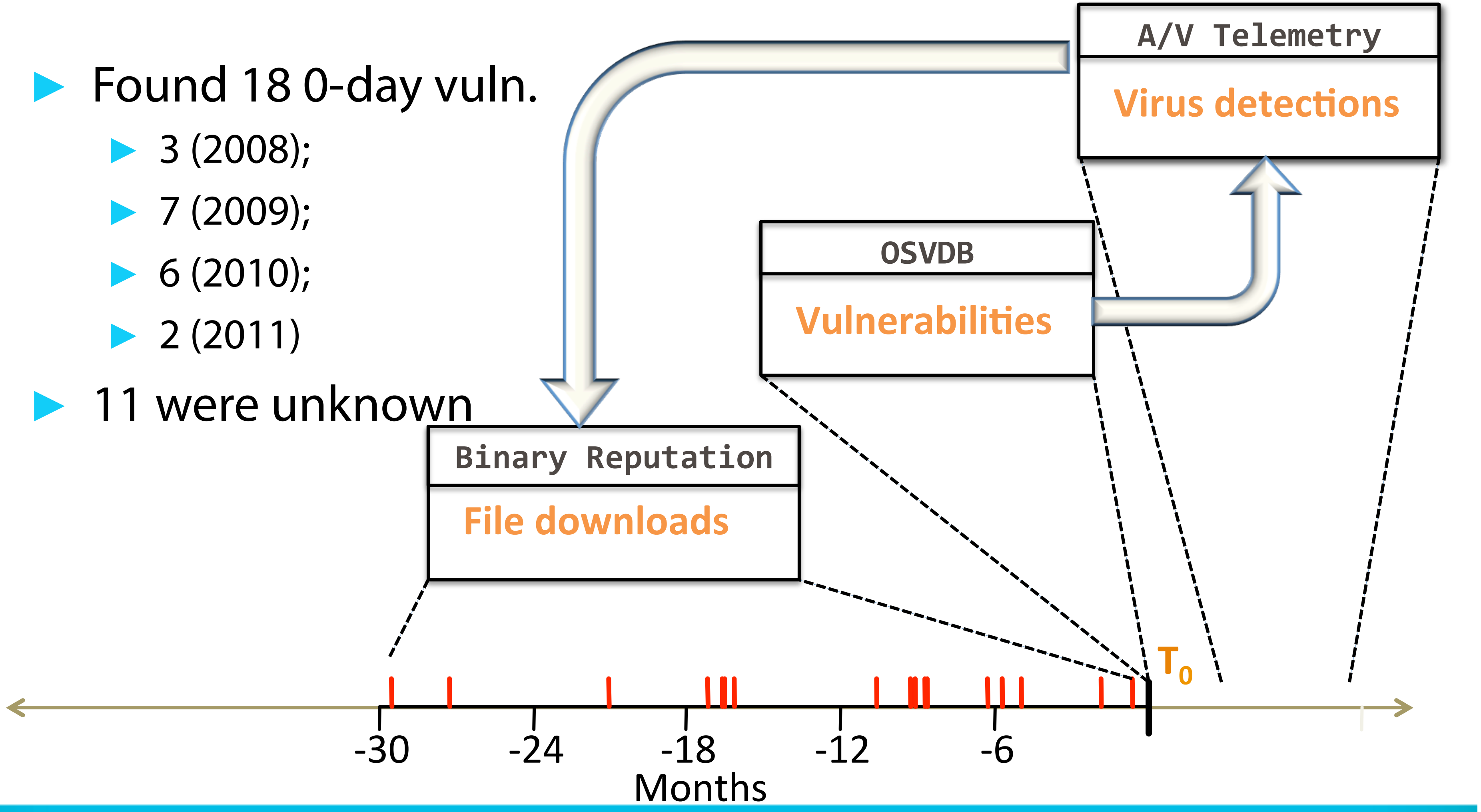
René Magritte (1898-1967)

Methodology



Results

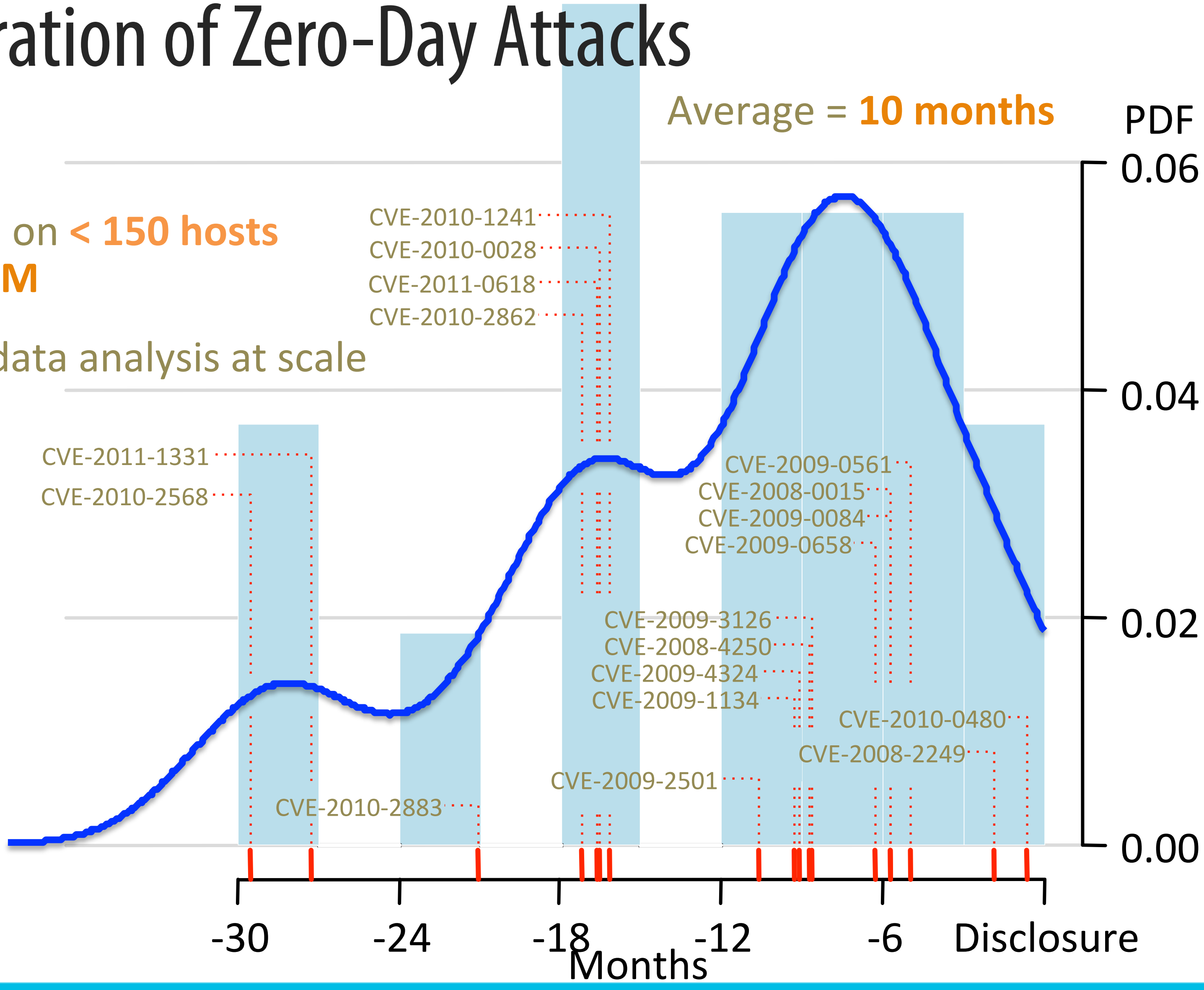
- Found 18 0-day vuln.
  - 3 (2008);
  - 7 (2009);
  - 6 (2010);
  - 2 (2011)
- 11 were unknown



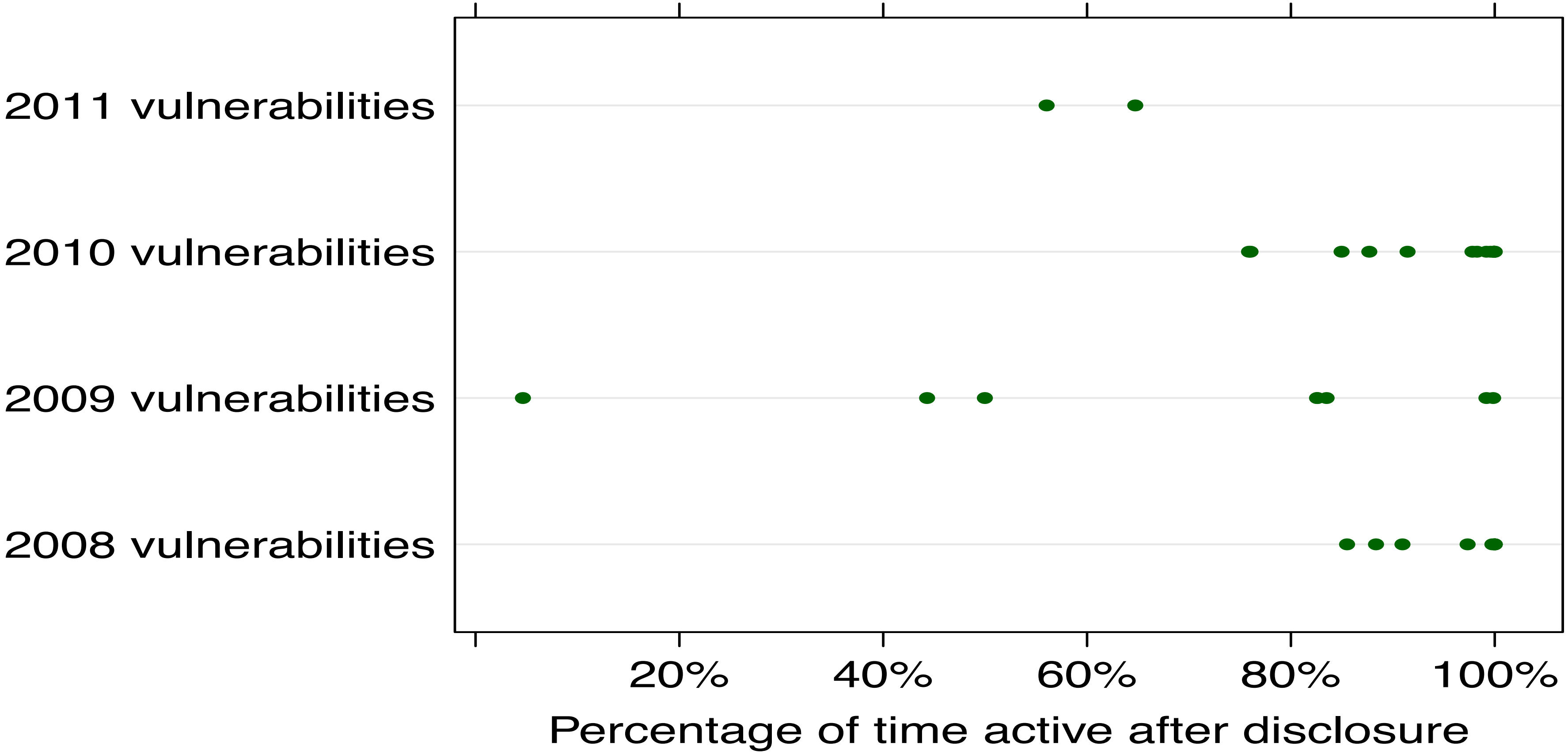
Duration of Zero-Day Attacks

Detected on **< 150 hosts** out of **11M**

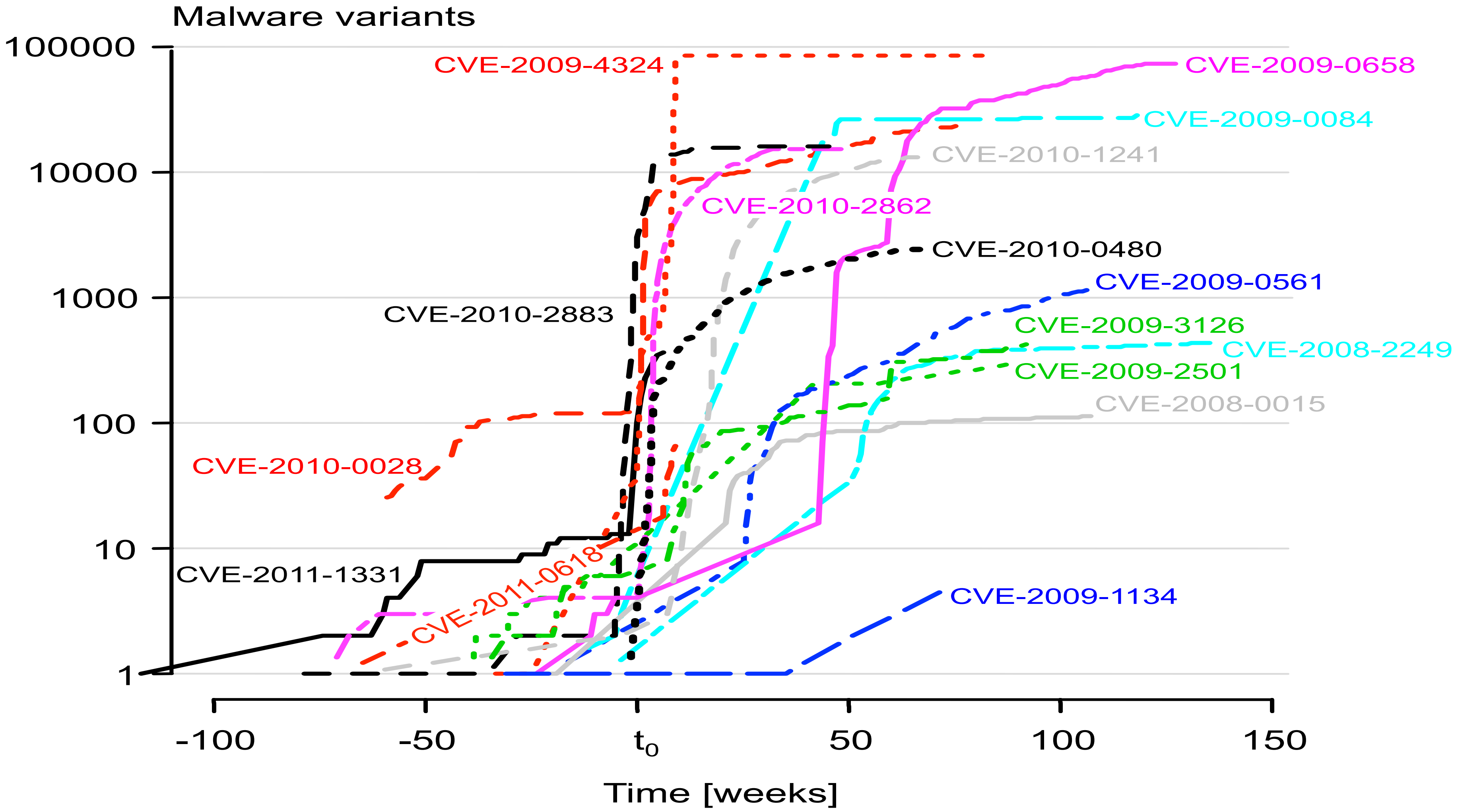
Require data analysis at scale



The usage of 0-day vulnerabilities after disclosure



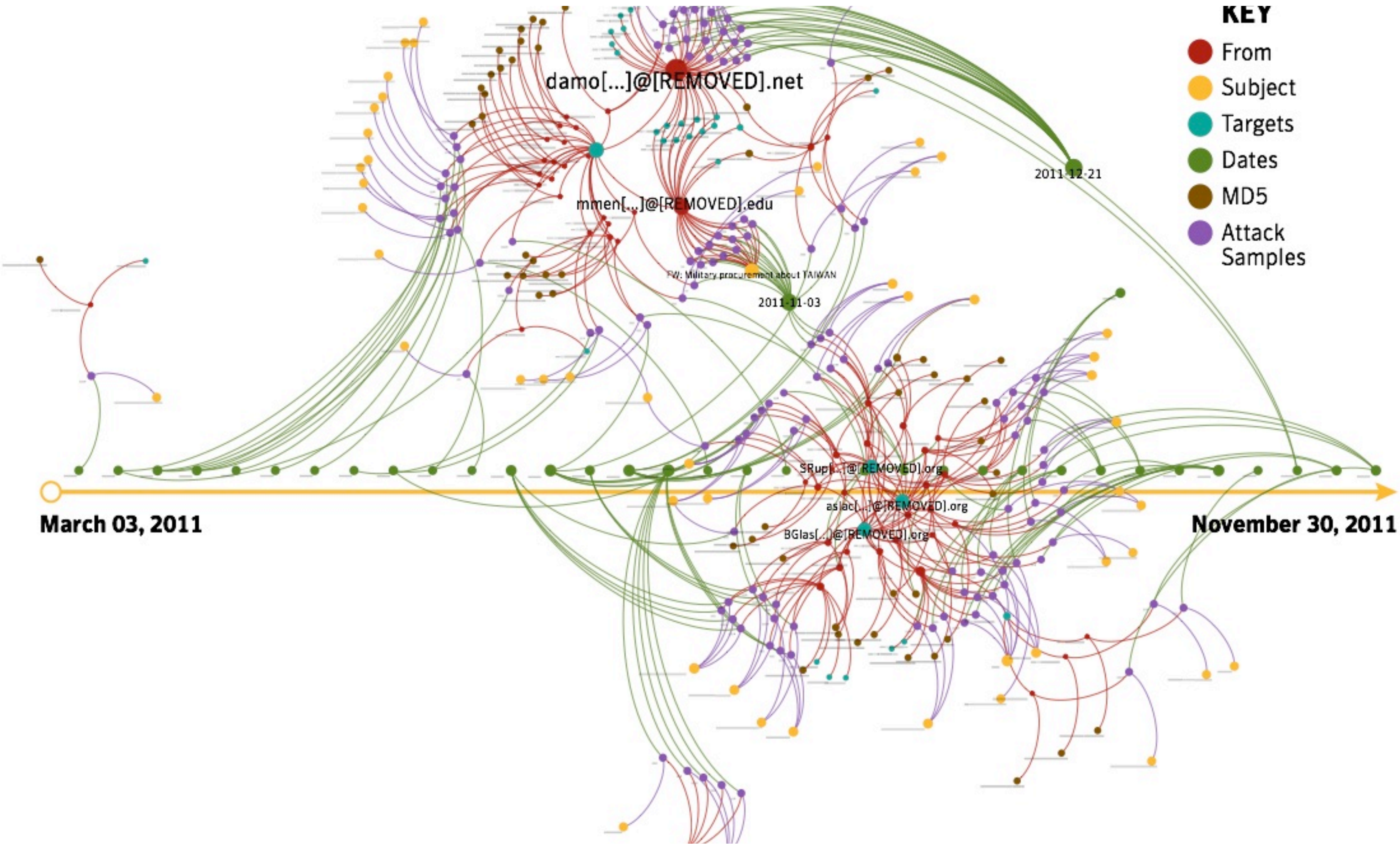
What happens after disclosure…



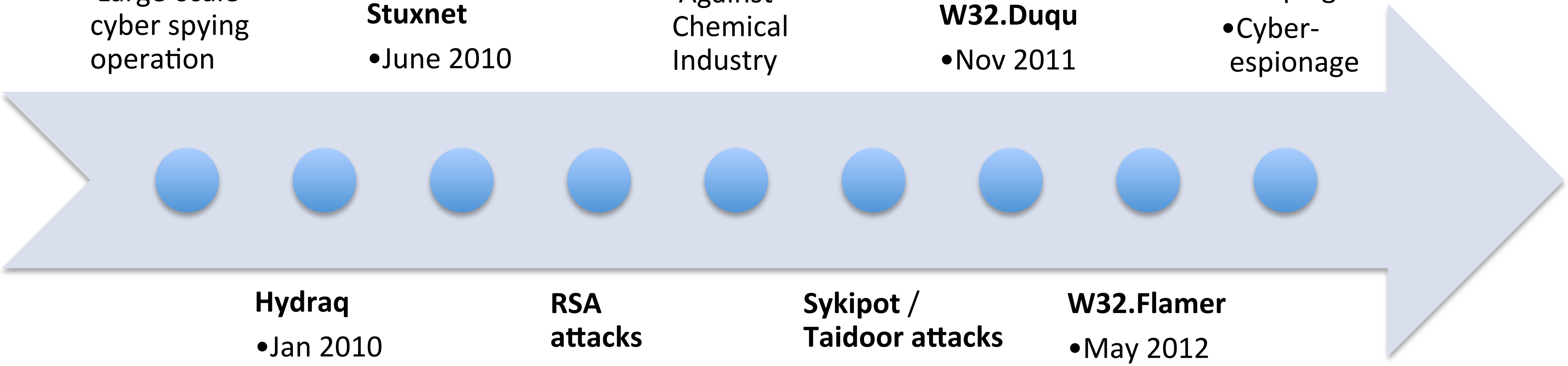
So … what ?

- Zero days remain hidden for a long time:
  - You have, quite likely, some in your organisation now!
  - Adopt a defense in depth approach and detect lateral propagation. Make the hacker's life difficult inside your network
- Vulnerabilities are being used for long period of times:
  - Patch all your systems, even the old ones, or shield them if you can't fix them.
- The disclosure of 0-day vulnerabilities lead to the creation of exploits that spread like wildfire
  - Have a very rapid and efficient "patching" process in place

Taidoor Attacks - 2011



Recent Evolution of Targeted Attacks



Ghostnet
- Mars 2009
- Large-scale cyber spying operation

Hydraq
- Jan 2010
- Operation "Aurora"

Stuxnet
- June 2010

RSA attacks
- August 2011

Nitro Attacks
- Jul-Oct 2011
- Against Chemical Industry

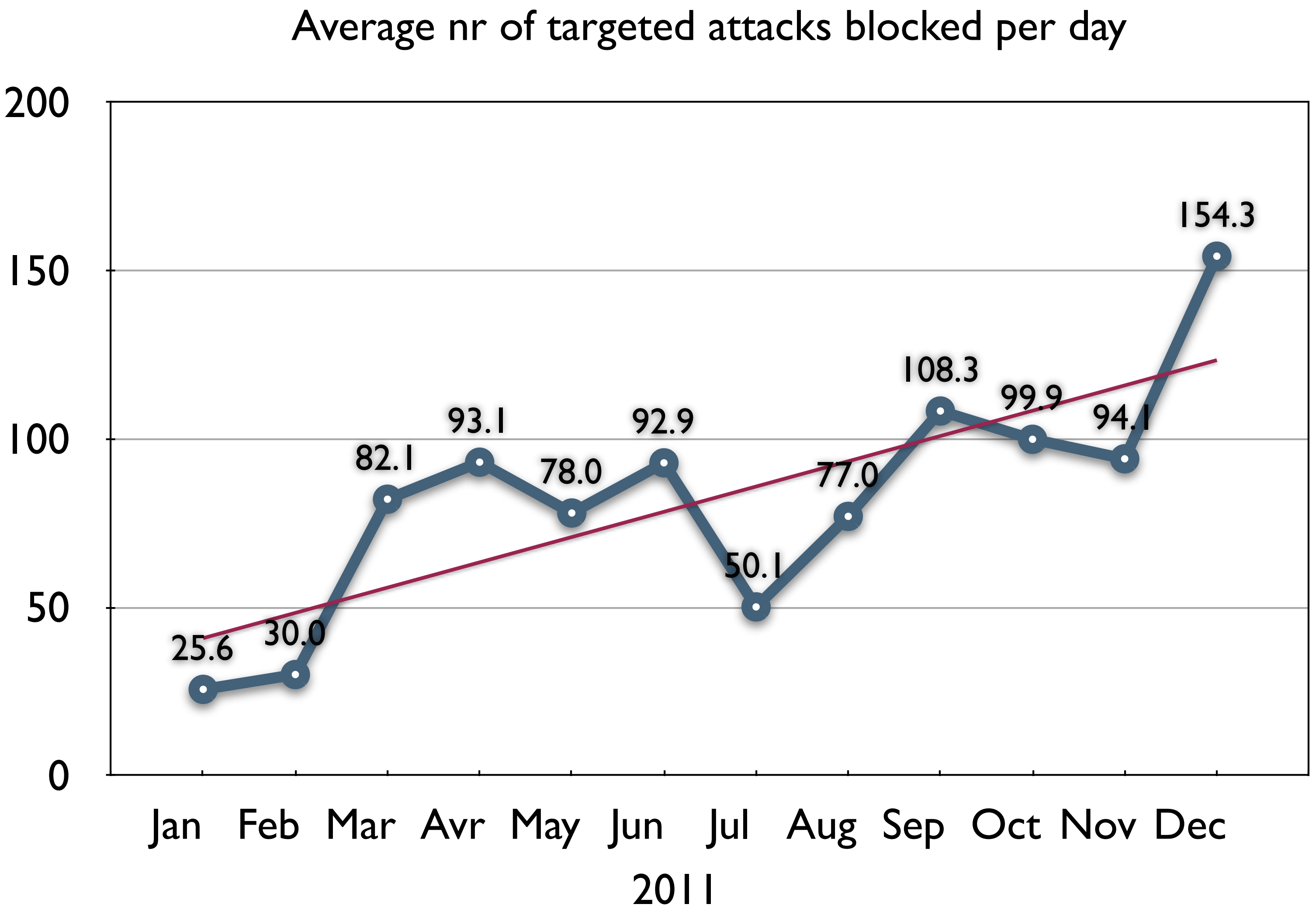
Sykipot / Taidoor attacks
- 2011
- Targeting Defense industry and Governments

W32.Duqu
- Nov 2011

W32.Flamer
- May 2012
- Highly Sophisticated Threat
- Targets the Middle East

Rocra – "Red October"
- Jan 2013
- Multi-year campaign
- Cyber-espionage

Rise in Targeted Attacks Activity in 2011



Limitations

Web attacks

Polymorphism

Exploits in non-executable files

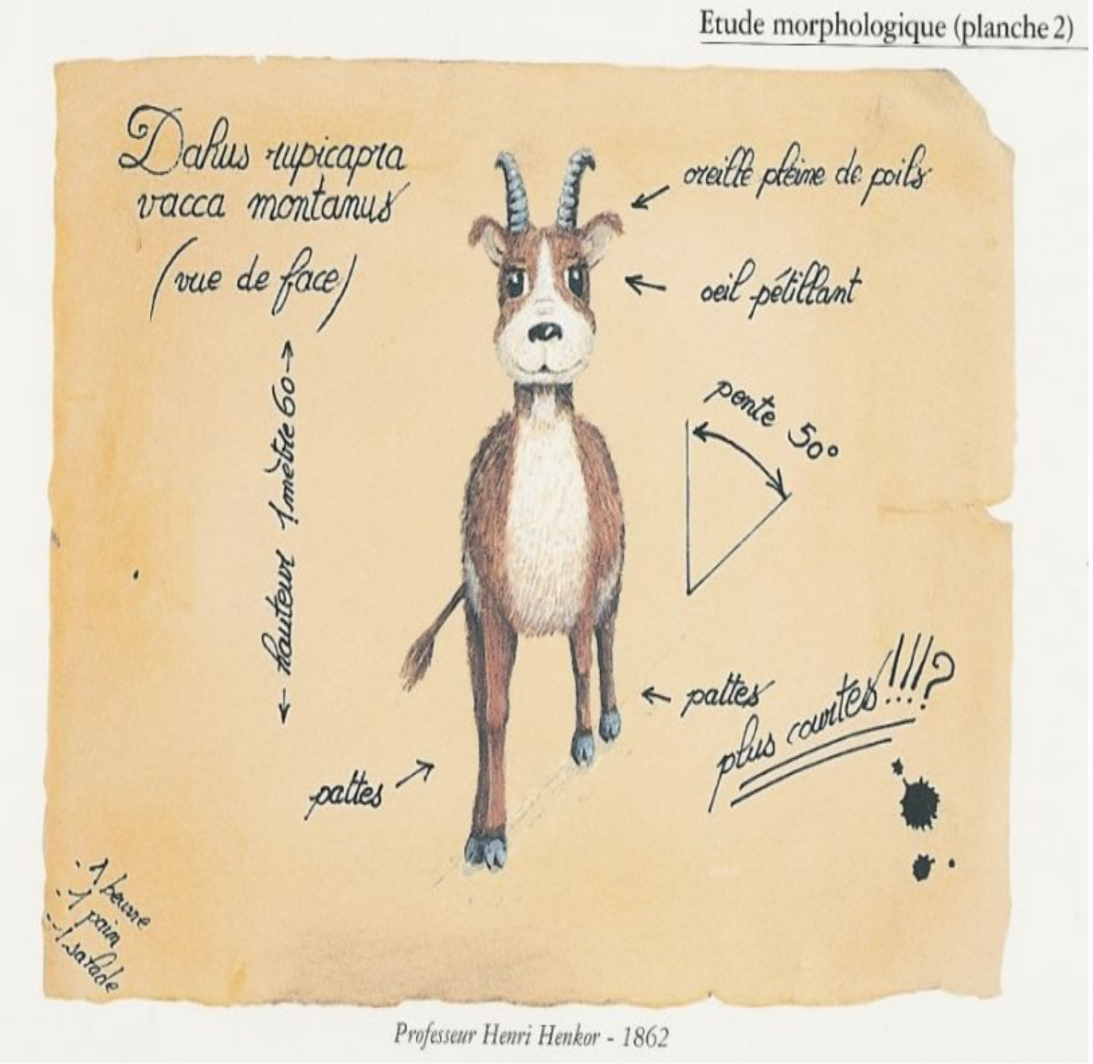
Highly Targeted Attacks

Dahu: Definition

- “The Dahu is an extremely shy animal living in the Alps of France and Switzerland.[…] It has adapted to its steep environment by having legs shorter on the uphill side and longer on the downhill side […] “

“The Dahu, An endangered Alpine species”,
Science, 2568, November 1996, pp.112,
www.vidonne.com/html/dahu-reignier.htm

Dahu


Etude morphologique (planche 2)
Dahus rupicapra vacca montanus
(vue de face)
oreille pleine de poils
oeil pétillant
pente 50°
← hauteur 1 mètre 60 →
pattes
pattes plus courtes!!!?
1 beurre
1 pain
1 salade
Professeur Henri Henkor - 1862

Food for thoughts

- Dahus are rare, bizarre, stimulating from an intellectual point of view but ...
  - Does it justify the existence of *Dahusian research*?
  - How can we make sure we are not building tools against *Dahusian hackers*?
  - How can we avoid (re)inventing *Dahusian solutions*?

Conclusions

- Using data collected from real users, we were able to find 18 zero-day vulnerabilities
- Zero-day attacks last between 19 days and 30 months, with a median of 8 months and an average of approximately 10 months
- The public disclosure of vulnerabilities is followed by an increase of up to five orders of magnitude in the volume of attacks
- To decrease the window of exposure, software vendors should be more careful to provide patches and make sure everyone applies them