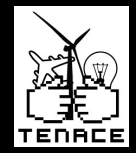
UNIVERSITY OF TRENTO



MalwareLab: Experimentation with Cybercrime Attack Tools

Luca Allodi, Vadim Kotov, Fabio Massacci
University of Trento, Italy
http://disi.unitn.it/~allodi

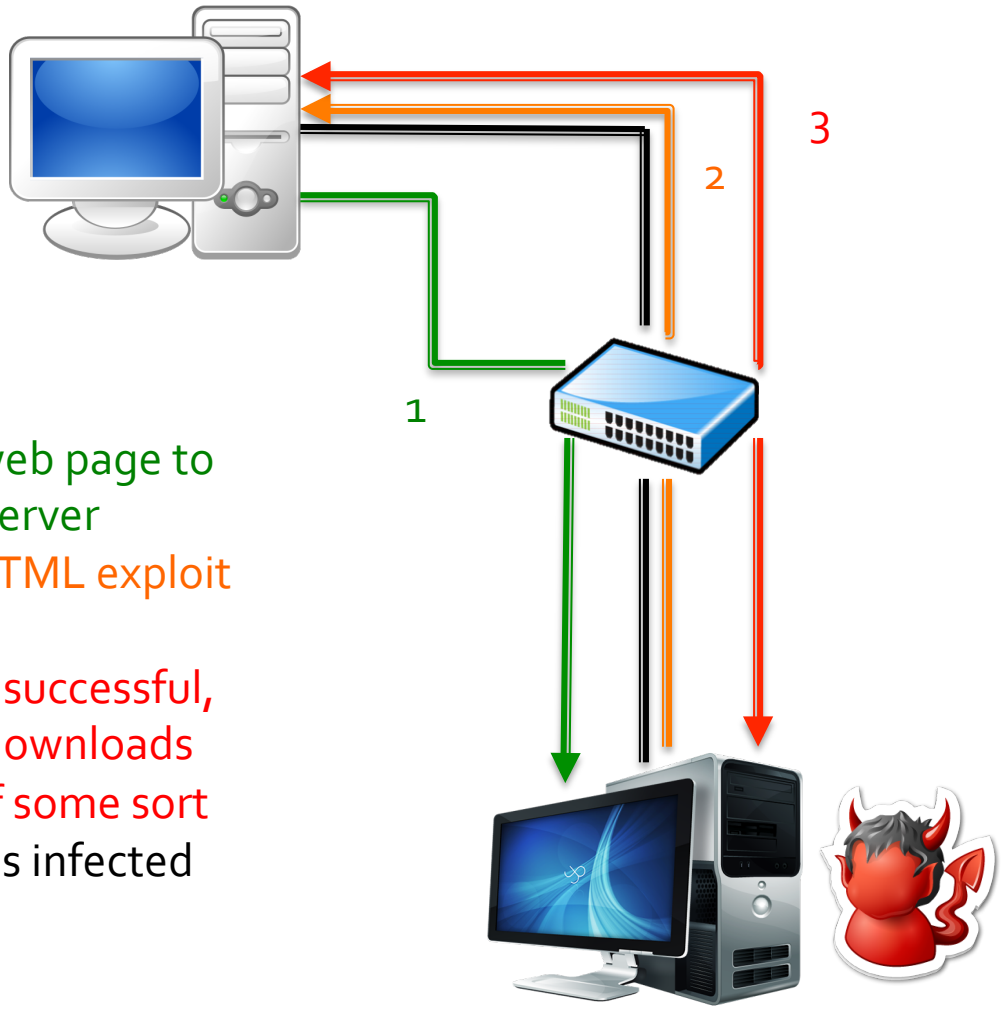
Outline

- MalwareLab: What we tested for
- How do exploit kits work
- How we perform the experiment
- The experimental infrastructure
- Results
- Conclusion & lessons learned

MalwareLab: What we tested for

- MalwareLab at the University of Trento, Italy
  - Platform to test malware products as "software artifacts"
- In this work we tested 10 exploit kits to answer the following question:
  - *How resilient are Exploit Kits against software updates?*

How do exploit kits work



1. Requests web page to malicious server
2. Receives HTML exploit page
3. If exploit is successful, shellcode downloads malware of some sort
4. Computer is infected

SECONOMICS

TENACE

How we perform the experiment

- Limits for realistic configurations:
  - Window-life of an operating system:
    - 6 years
  - Window for co-existence of software:
    - 2 years
  - Lots of sw out there → as commercial products Exploit Kits must be able to deliver in a variety of circumstances
- What we test
  - Exploit kit resiliency against evolving software configurations
- What we measure
  - Successfulness of the exploitation (execution of our "malware" across evolution of victim configurations)

The Kits and The Victims

- Exploit kits span from (2007-2011)
  - How we chose the exploit kits
    - Release date
    - Popularity (as reported in industry reports)
    - CrimePack, Eleonore, Bleeding Life, Shaman, …
- Software: most popular one
  - Windows XP, Vista, Seven
    - All service packs are treated like independent operating systems
  - Browsers: Firefox, Internet explorer
  - Plugins: Flash, Acrobat Reader, Java
- 247 software versions
  - spanning from 2005 to 2013
- We randomly generate 180 sw combinations (x9 Operating Systems) to be the configurations we test
- Manual Test is Impossible → we need an automated platform

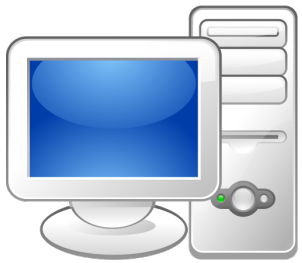
SECONOMICS

Configuration example

- One configuration for: Windows XP Service Pack 2
  - Firefox 1.5.0.5
  - Flash 9.0.28.0
  - Acrobat Reader 8.0.0.0
  - Quicktime 7.0.4.0
  - Java 1.5.0.7
- One configuration for: Windows Seven Service Pack 1
  - Firefox 8.0.1.0
  - Flash 10.3.183.10
  - Acrobat Reader 10.1.1.0
  - Quicktime: No version
  - Java 6.27

The experimental Infrastructure

Virtualizes:
- XPSP0
  - Conf 1..180
- XP SP1
  - Conf 1..180
- XP SP2
  - Conf 1..180
- XPSP3
  - Conf 1..180



Virtualizes
- Vista SP0
  - Conf 1..180
- Vista SP1
  - Conf 1..180
- Vista SP2
  - Conf 1..180

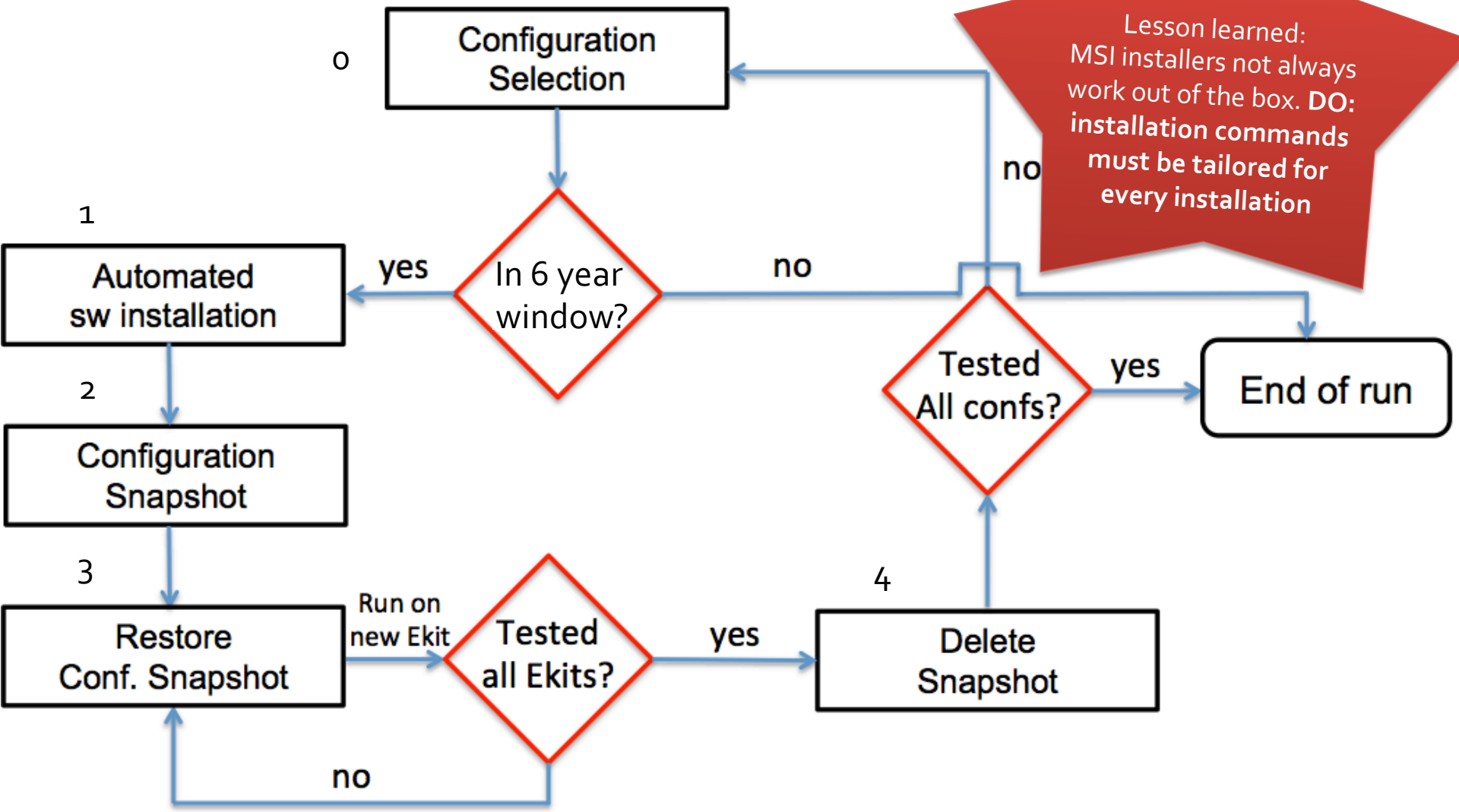
Virtualizes
- Seven SP0
  - Conf 1..180
- Seven SP1
  - Conf 1..180

Lesson Learned:
Experiment runs can fail for unexpected reasons. **DO: keep track of the infrastructure state to restore it at the moment of failure, even if only one machine failed.**

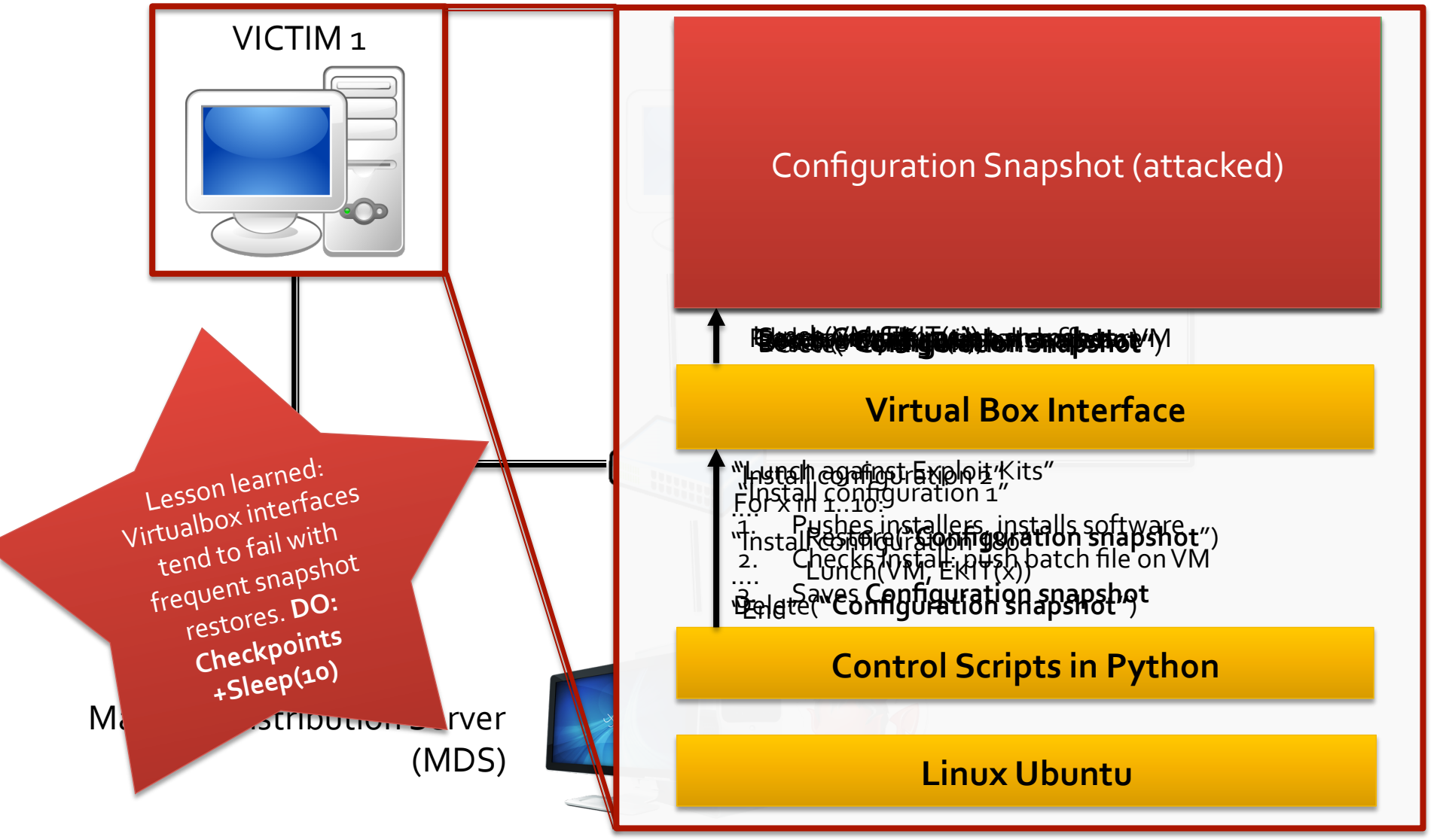
- Exploit kit 1
- Exploit kit 2
- ..
- Exploit kit 10

Malware Distribution Server (MDS)

Overview of the experiment



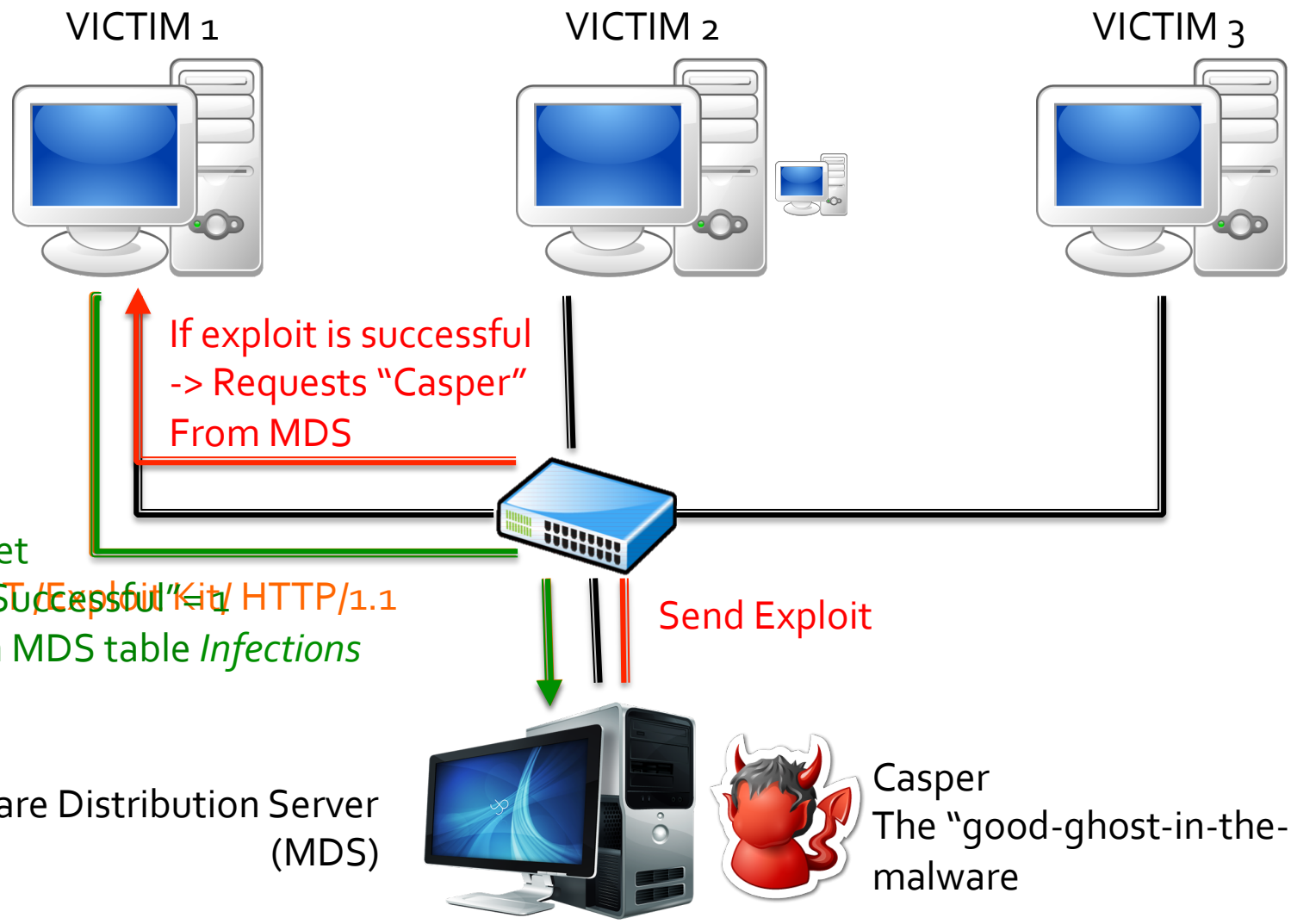
The experiment: VICTIM



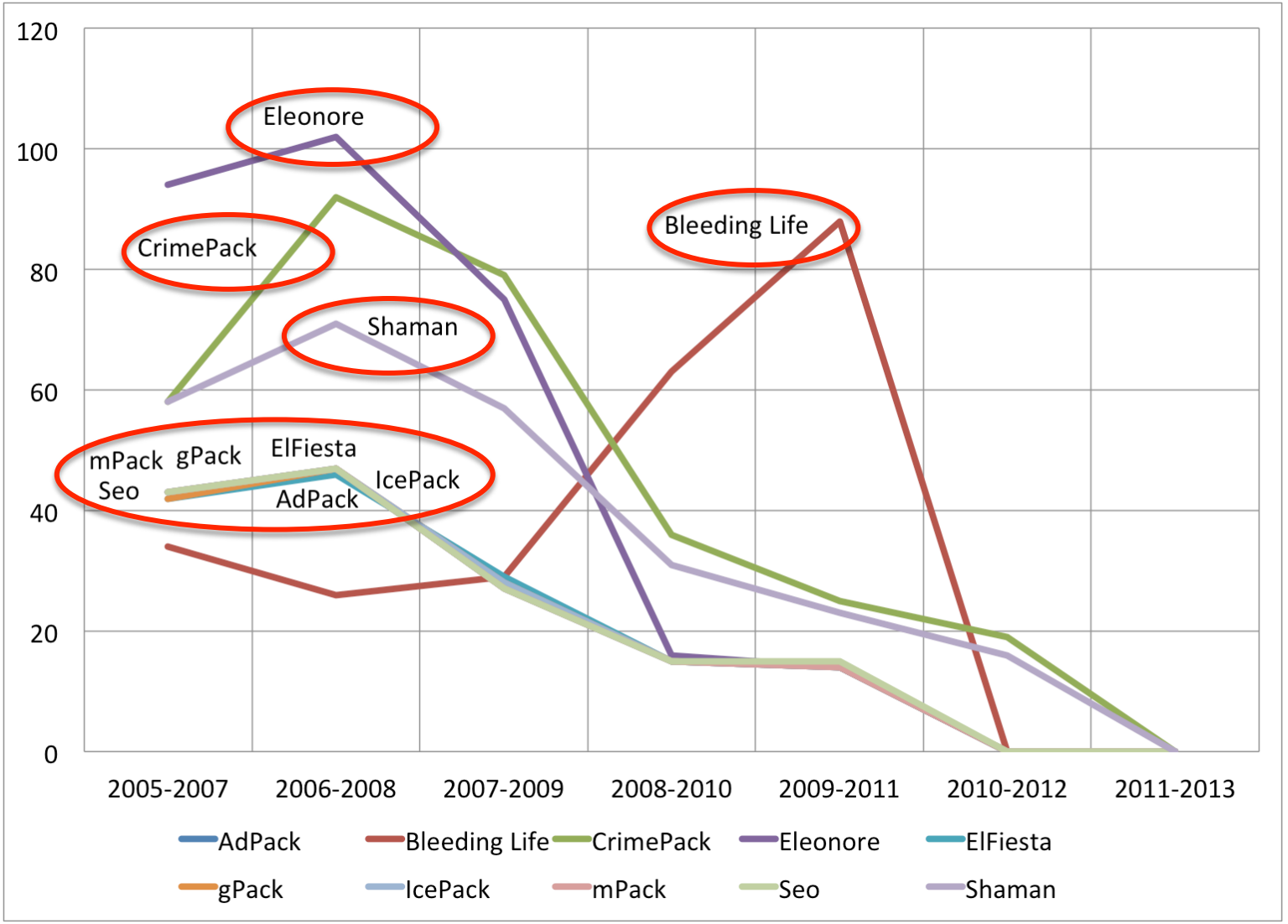
Assessing VICTIM configurations

- Installed configurations must be checked because exploits may fail for two reasons:
  - Vulnerable software is not there
  - Exploit kit software is bad
- How do we measure if an installation is successful?
  - Check for existence of known post-installation files on file system
    - May still have false positives, false negatives
- Most software installation were marked "successful"
  - Java, Acrobat, Firefox, all successful
  - Flash failed for 20% of installations
- Better suggestions are welcomed

Assessing exploit successes



Results: Infection I



Results of the experiment

- Exploit kits are armed differently to either:
  1. *Short-term kits:* Guarantee maximum infections in short periods of time
  2. *Long-term kits:* Enhance proficiency in time
  3. *Lousy kits:* "borrow" exploitation code from other products

SECONOMICS

Summary of lessons learned

- Experiment runs can fail for unexpected reasons. **Make checkpoints to restore the infrastructure state.**
- MSI installers not always work out of the box. **Installation commands must be tailored for every installation.**
- Virtualbox interfaces tend to fail with frequent snapshot restores. **Use checkpoints and slow down sequential snapshot restores.**

Questions?

- Luca Allodi
luca.allodi@unitn.it

- Vadim Kotov
cons_vkotov@bromium.com

- Fabio Massacci
fabio.massacci@unitn.it