UNIVERSITY OF TRENTO

SECONOMICS

Knowing the attackers

Governmental Malware and Cybercrime

An Overview

Luca Allodi
University of Trento, Italy.
$name.$surname@unitn.it

Knowing the attackers: outline

- Overview of cybersecurity players
  - The defenders: The vendors and the system administrators
  - The attackers:
    - Target-oriented attackers: Governments and Agencies
    - Mass attackers: Cybercrime
- Cybercrime: a techno-economic overview
  - How are black markets configured?
  - I'll tell you a few stories. Key-points:
    - What makes a market a good market
    - How are trades organized
    - How is punishment enforced (for cheaters, rippers)
- Hans-on report on Cybercrime tools

The defenders: in a nutshell

- Vendors produce software with vulnerabilities
  - Vulnerability = software flaw that can be exploited to attack a system
- System administrators have to manage their systems to make them secure
  - Hardening (software configuration)
  - Infrastructural security (e.g. firewalls, de-militarized zones, etc)
  - Compliance, etc.
- Who is going to attack me and how will he attack me?

The attackers: Target-oriented

- These attackers are the hardest to defend against
  - They have competitive advantage
    - They usually know more about your system that you do (zero-day vulns)
    - Well-financed or highly motivated
- Advanced Persistent Threats (APTs)
- Governmental malware is a good example
  - Used by governments to control and monitor "suspects"
    - E.g. anti-terrorism programs, drug dealers in Silk Road
  - Several agencies provide governments with "ad-hoc" attacks
    - VUPEN (France)
    - Hacking Team (Italy)
    - Gamma International (UK)
  - Sometimes attacks are internally developed

Target-oriented example: FinFisher

- FinFisher is a recent example of controversial governmental malware provided by an external agency
- Developed by Gamma International
  - Revealed by independent researchers
- Has been used to
  - Contrast governmental opposition or rebellion
    - Egypt, Bahraini
  - Unclear surveillance purposes
    - Germany, Ethiopia
- What does it do
  - Monitors victims' computer
  - Capable or recording emails, Skype audio and video conversations, using webcams, etc.
- → https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/

Mass attacks: Cybercrime

- Other attackers are not focused on one particular target (e.g. a rebel)
- Their goal is to gain control over a victim's systems to pursue criminal actions
  - Stealing data
  - Credit Cards, SSNs, Spam
  - Turning systems into bots
  - Using computation power to break crypto
  - …
- These attacks are by far the most common
- Organized in market systems ← our focus today

SECONOMICS

TENACE

What is a market

- A market is a *system* in which services or goods are traded in exchange of a compensation
- There can be many types of markets
  - Financial markets
  - Work / Job position markets
  - ..
- A marketplace is a venue where the market is held
  - Physical (a town’s square)
  - Virtual (a website, a chat, other or mixed means)
  - The terms “market” and “marketplace” will be used interchangeably in this lecture

SECONOMICS

TENACE

What are the (cybercrime) black markets

- Held in virtual marketplaces
  - Originally IRC
  - Now mostly web-forums
- Trading of
  - Attacking tools
  - Highly efficient exploits; Vulnerabilities
  - Accounts, money laundry, CCNs..
- We encountered two types of black markets:
  - Open -> anyone can freely access, no barriers
    - Example are IRC markets for CCNs
    - These markets have been shown to be strongly "unfair"
  - Segregated -> language barriers and/or pull-in mechanisms
    - If you don't speak Russian/Chinese you are not welcome
    - Lately language barrier has been also integrated by a "interview" to get access to the marketplace

Black Markets: Why should we care?

- How many of you drive..?
  - Have ever took a flight..?
  - Make phone calls..?
  - Eat..?
- How many of you can build a car?
  - Build an airplane?
  - Build a phone?
  - Cook (warming pizza up does not classify as cooking)?

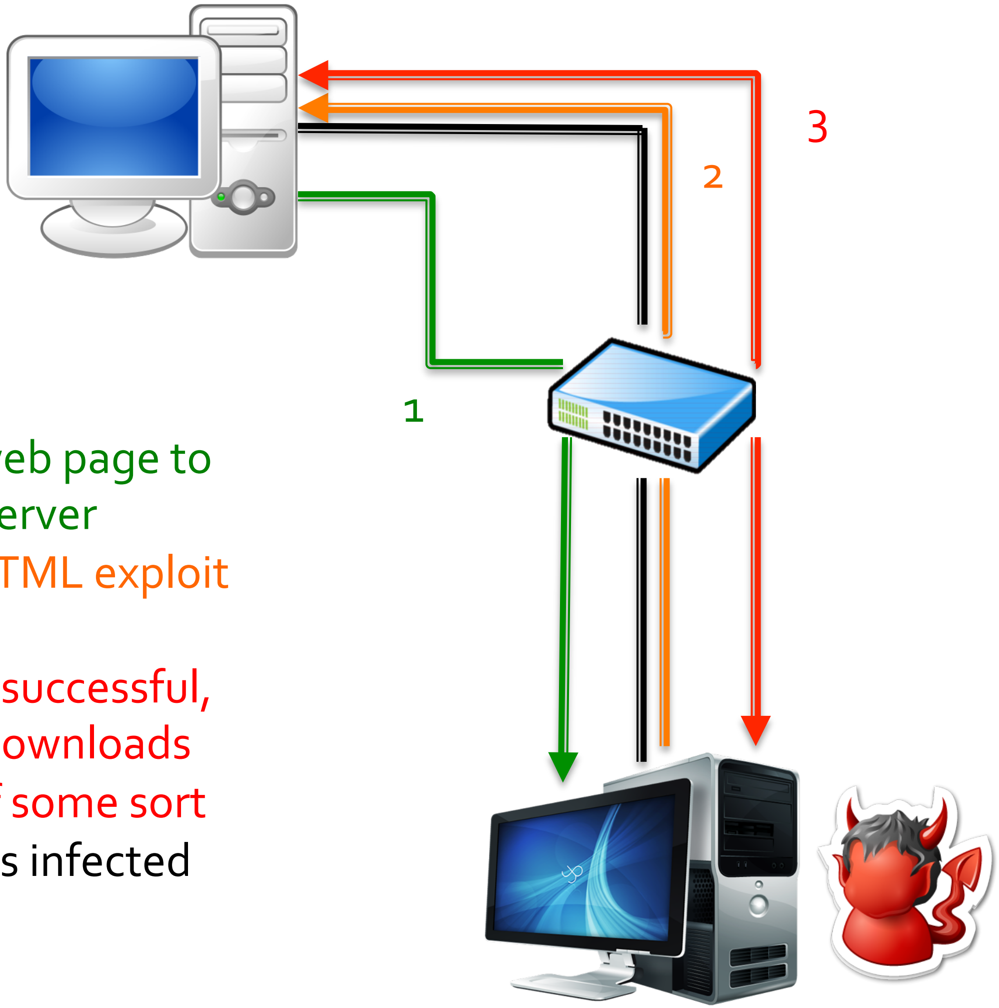
- → One of markets' primary functions is to *outsource* technicalities to third parties that deliver a final product that can be used *out-of-the-box*

Black Markets: Why should we care?

- How many of you can build an actual exploit and delivery mechanism that
  - Freshly encrypts all its instances to decrease AV detection rates
  - Reliably executes its shellcode avoiding ASLR/DEP
    - E.g. Employs advanced return-oriented-programming techniques
  - Reliably delivers an encrypted payload
    - That silently installs on the victim machine
    - And returns the control to the parent process without having it throwing any exceptions?

- Commoditization of attacks greatly increases attackers capabilities
- With 10.000$ US$/yr you can build a 1M bots botnet
  - And to break even you need to get 1 US$ cent out of each.
  - You do not believe me?

Our case study:Exploit Kits:Model

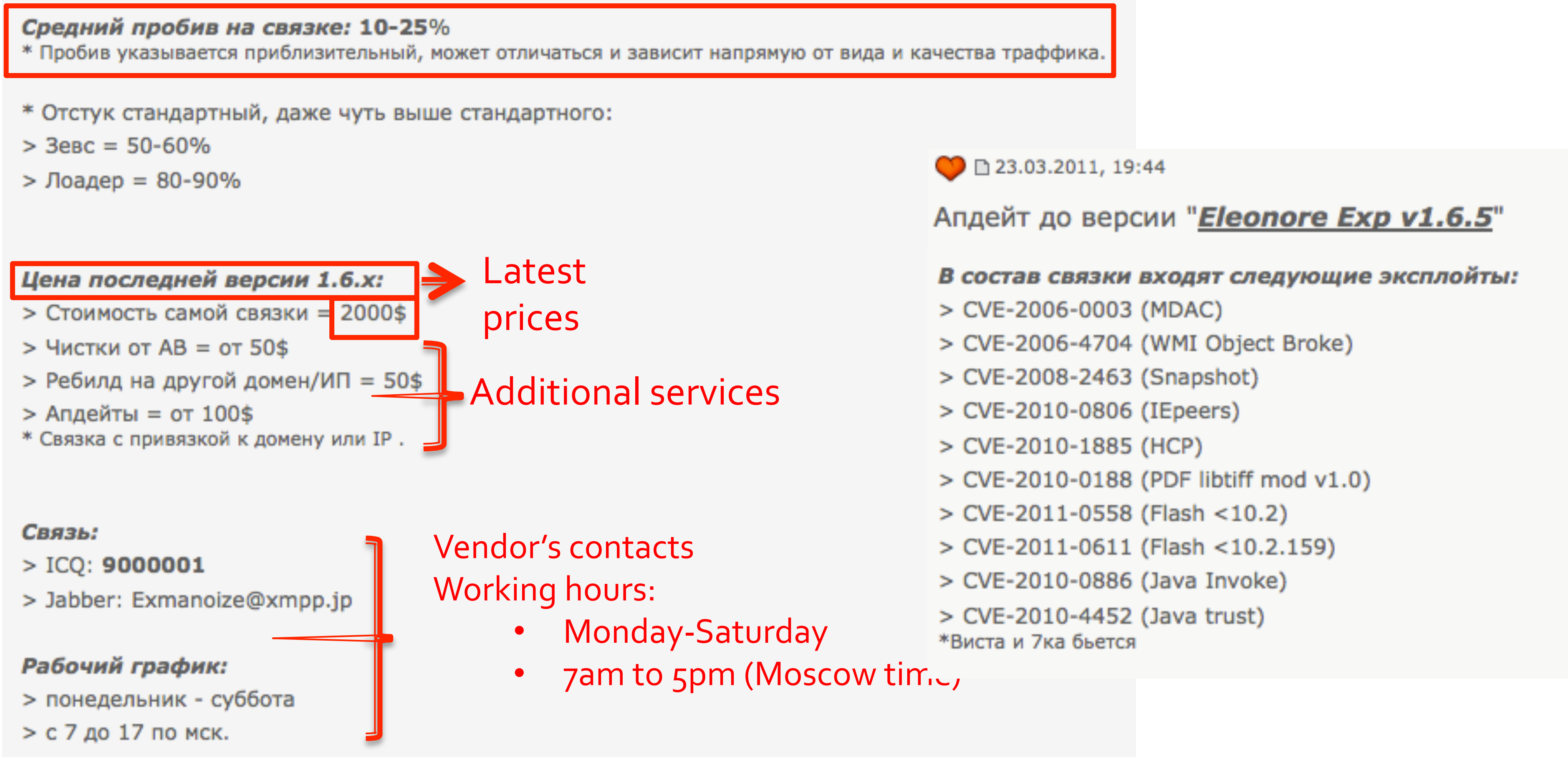


1. Requests web page to malicious server
2. Receives HTML exploit page
3. If exploit is successful, shellcode downloads malware of some sort
4. Computer is infected

Our case study:Exploit Kits:ads

Exploitation success rate

*Rate highly depends on traffic quality



Средний пробив на связке: 10-25%

* Пробив указывается приблизительный, может отличаться и зависит напрямую от вида и качества траффика.

* Отстук стандартный, даже чуть выше стандартного:

> Зевс = 50-60%

> Лоадер = 80-90%

Цена последней версии 1.6.x:

> Стоимость самой связки = 2000$

> Чистки от АВ = от 50$

> Ребилд на другой домен/ИП = 50$

> Апдейты = от 100$

* Связка с привязкой к домену или IP .

Latest prices

Additional services

Связь:

> ICQ: **9000001**

> Jabber: Exmanoize@xmpp.jp

Рабочий график:

> понедельник - суббота

> с 7 до 17 по мск.

Vendor's contacts

Working hours:

- Monday-Saturday
- 7am to 5pm (Moscow tim

23.03.2011, 19:44

Апдейт до версии "**Eleonore Exp v1.6.5**"

В состав связки входят следующие эксплойты:

> CVE-2006-0003 (MDAC)

> CVE-2006-4704 (WMI Object Broke)

> CVE-2008-2463 (Snapshot)

> CVE-2010-0806 (IEpeers)

> CVE-2010-1885 (HCP)

> CVE-2010-0188 (PDF libtiff mod v1.0)

> CVE-2011-0558 (Flash <10.2)

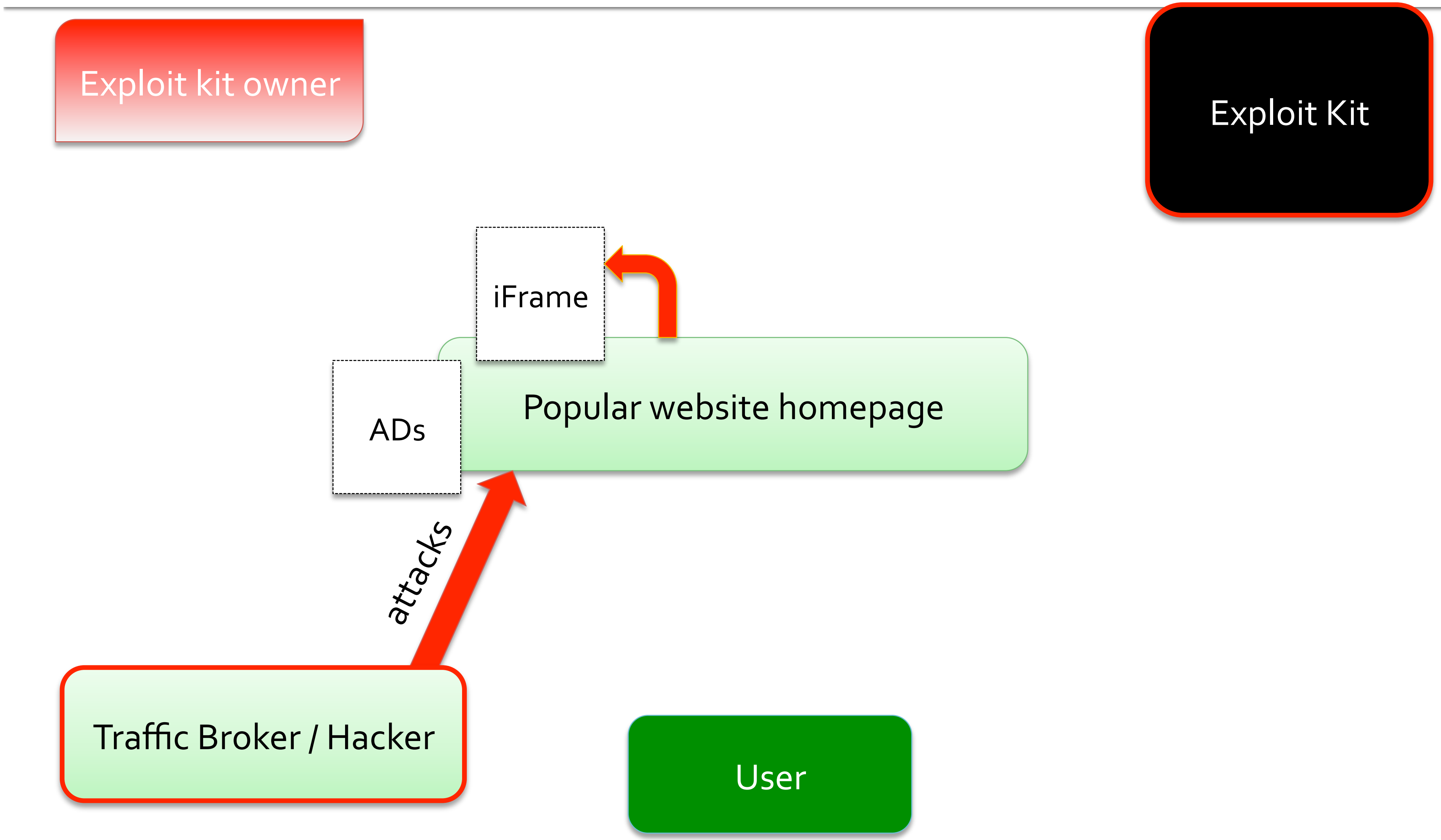
> CVE-2011-0611 (Flash <10.2.159)

> CVE-2010-0886 (Java Invoke)

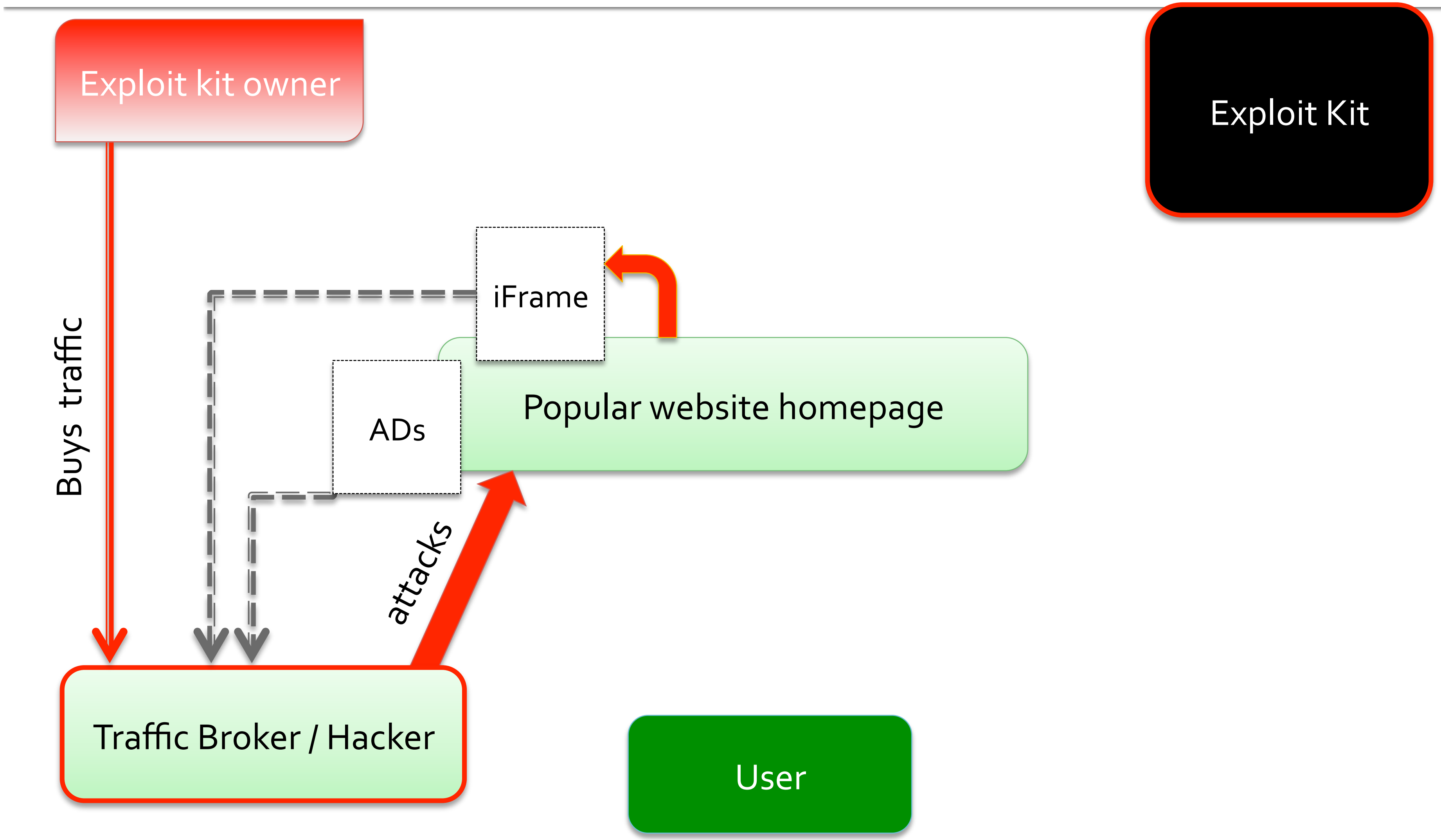
> CVE-2010-4452 (Java trust)

*Виста и 7ка бьется

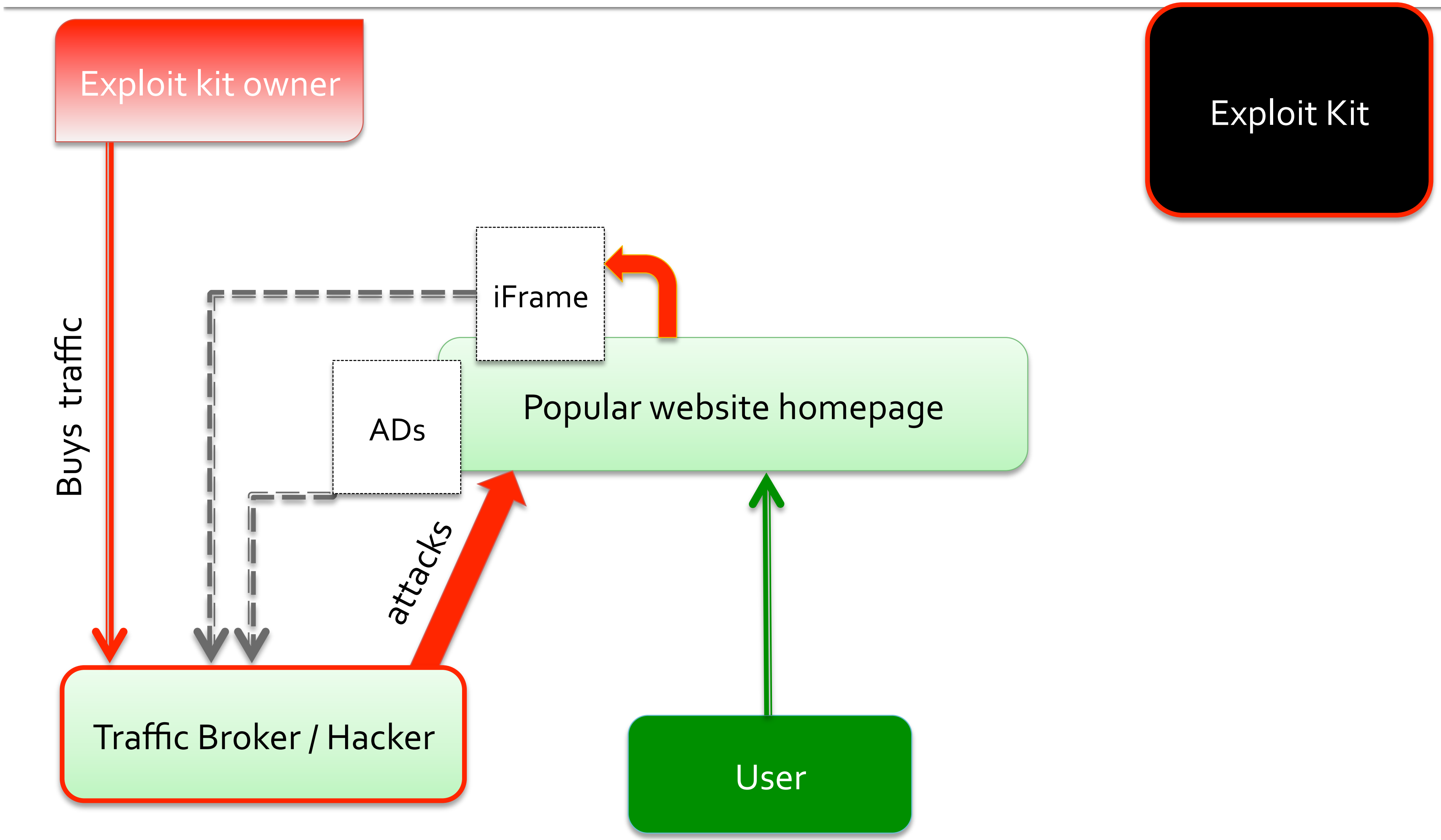
Exploit kits: a more complete model



Exploit kits: a more complete model



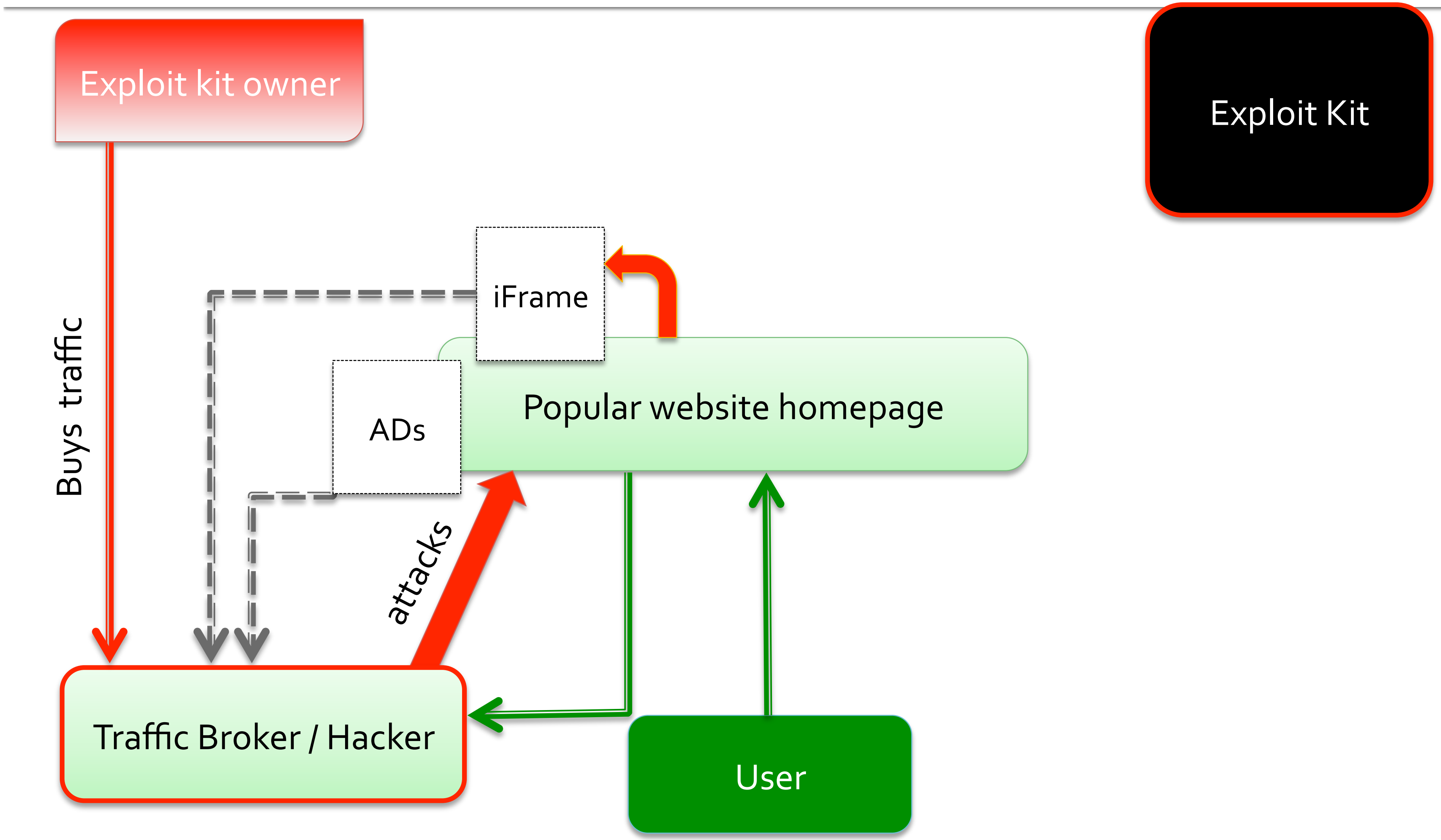
Exploit kits: a more complete model



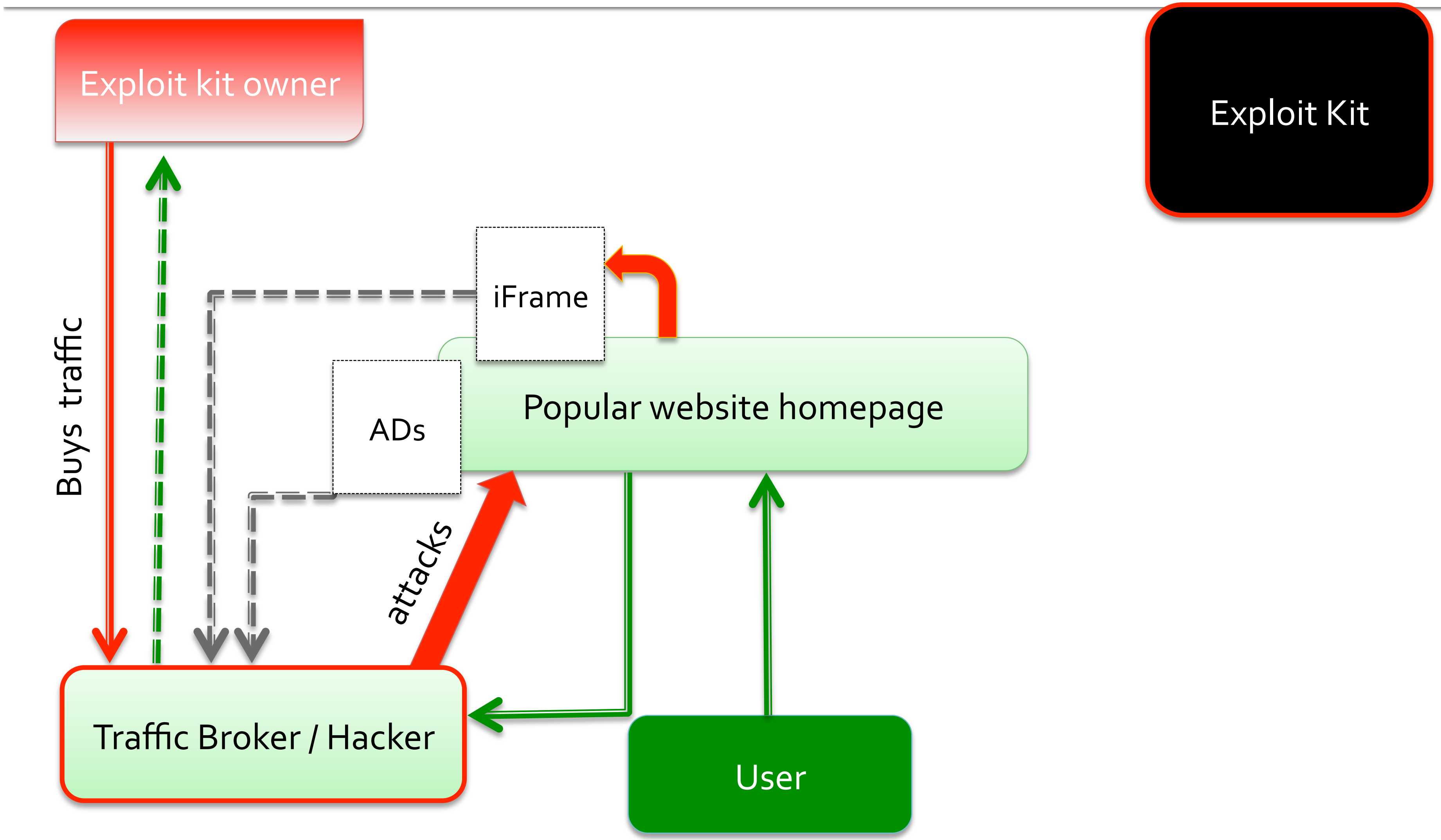
SECONOMICS

TENACE

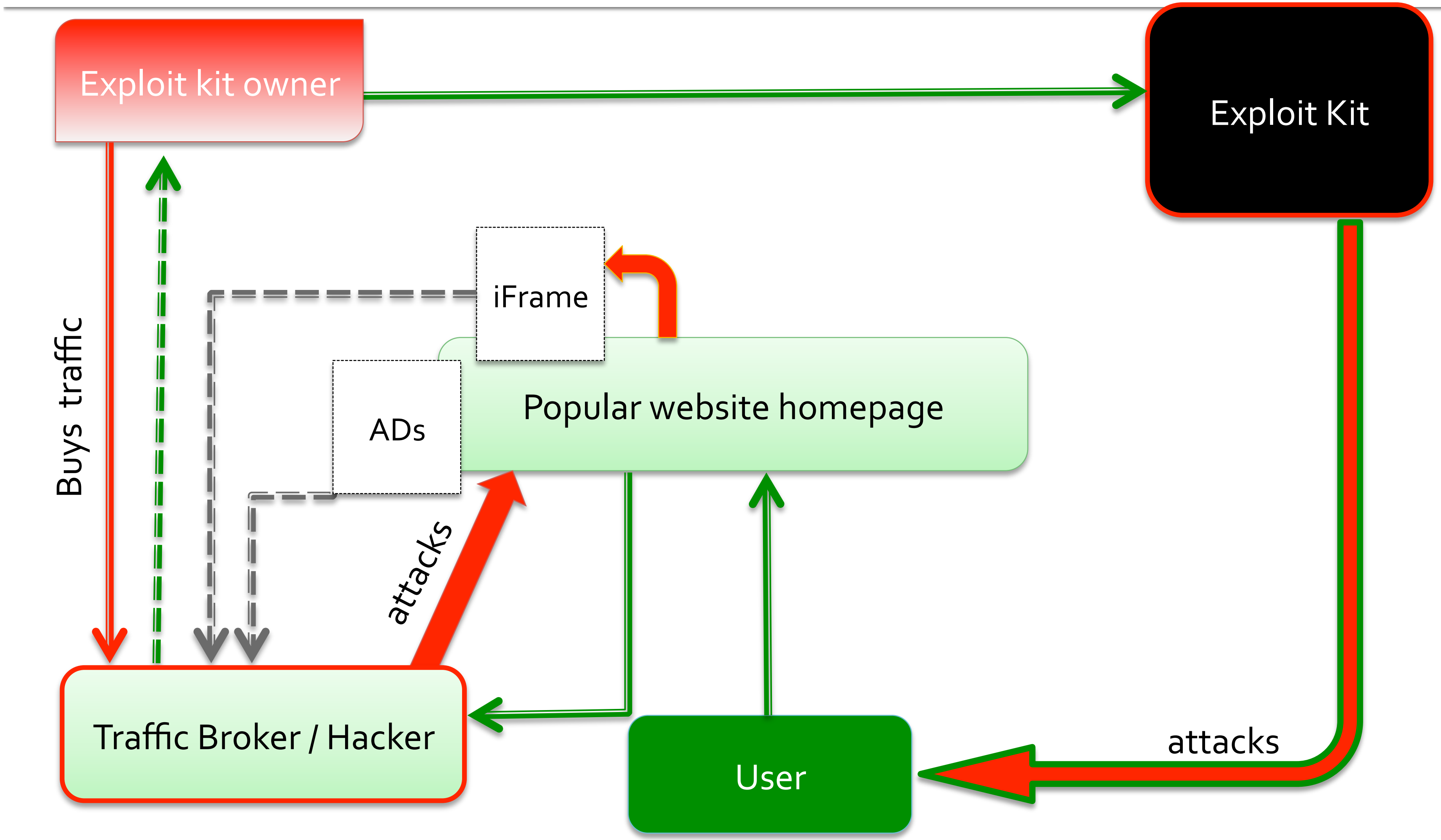
Exploit kits: a more complete model



Exploit kits: a more complete model

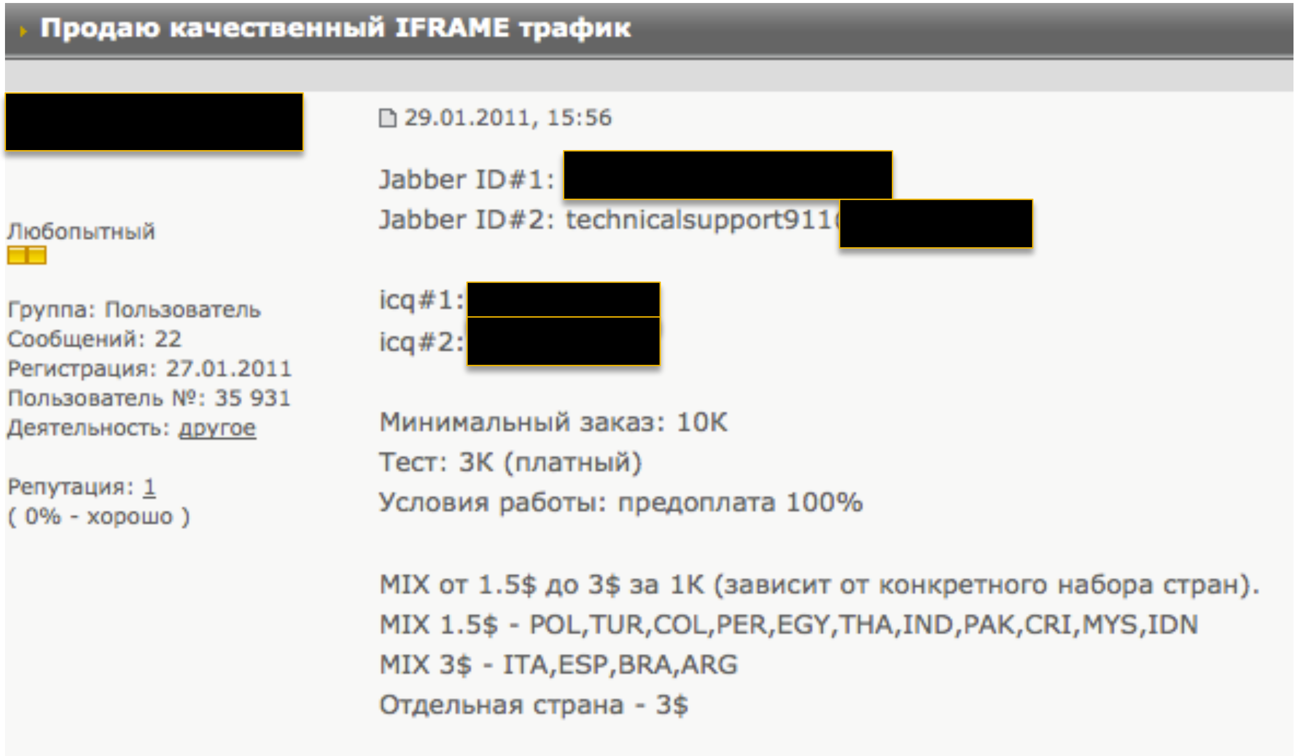


Exploit kits: a more complete model



Exploit kits: a more complete model

- Cybercrooks buy traffic from other crooks or online services (Ads network)
- High traffic quality means the cybercrook gets connections from the vulnerable systems he/she was looking for



▸ Продаю качественный IFRAME трафик

[redacted]

Любопытный

Группа: Пользователь
Сообщений: 22
Регистрация: 27.01.2011
Пользователь №: 35 931
Деятельность: другое

Репутация: 1
(0% - хорошо)

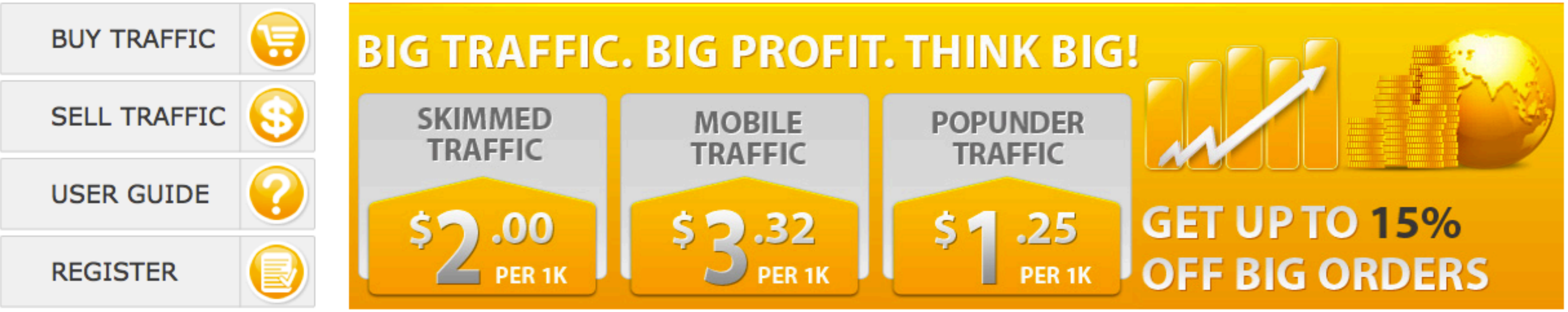
29.01.2011, 15:56

Jabber ID#1: [redacted]
Jabber ID#2: technicalsupport911[redacted]

icq#1: [redacted]
icq#2: [redacted]

Минимальный заказ: 10K
Тест: 3K (платный)
Условия работы: предоплата 100%

MIX от 1.5$ до 3$ за 1K (зависит от конкретного набора стран).
MIX 1.5$ - POL,TUR,COL,PER,EGY,THA,IND,PAK,CRI,MYS,IDN
MIX 3$ - ITA,ESP,BRA,ARG
Отдельная страна - 3$



Costs of building a 1M bots botnet

Action	Economic effort (1st year)
Buy exploit kit (20% efficiency)	2000 USD
Number of needed connections for 1M infections	5×10^6
Buy Traffic (assuming 2USD/1k)	10.000 USD
Deployment	50-150 USD
Maintain (change IPs, clear logs..)	150 USD
Updates (assume 2/yr)	~ 200 USD
Total	**~ 12.400 USD – 12.500 USD**
Breakeven ROI/BOT	**~ 0.01 USD**

Yes but.. This guys are criminals, right?

- Criminals selling illegal tools to other criminals in a free market (in the sense of no taxes, no government control..)
  - Are we sure that those markets function properly?..
  - .. And are not reduced to a "wanna-be scammer scammed by a scammer" situation?
- The tools are reportedly in the wild and infect machines, so it looks like the markets work. But how?

The Principal-Agent problem

- In any market, there is a selection problem between the player that needs the service, and the player who offers it
- Think of a typical car scenario:
  - Your car brakes down
  - You do not know much about cars / do not have time to repair it yourself
  - You, the **Principal**, are willing to pay a mechanic, the **Agent**, to get the job done
- How do you choose the right agent for the job?
  - How do you assess the veridicality of his "diagnose"?
- How do you know that the agent is not going to scam you?
  - E.g. by loosening a bolt so that in 2-3 months you'll come back to him?

Information asymmetry

- This is called “information asymmetry” and is typical of many markets
- It has initially been shown by Akerloff et al. in 1970, for the “used cars market”
  - ***The Market for "Lemons": Quality Uncertainty and the Market Mechanism***
- It is apparent anytime the Principal and/or the Agent cannot make a decision based on complete (and therefore equal) information
  - E.g. you don’t know enough about cars to assess the mechanic’s work -> the Agent knows more than the Principal does

Information asymmetry

- Information Asymmetry can be analyzed in terms of
  - Adverse selection
  - Moral hazard

- Adverse selection
  - You are not picking up from the right “pool of agents”
- Moral hazard
  - The agents may have incentives to scam you and/or change their behavior after the contract is signed

SECONOMICS

TENACE

In other words

- Adverse selection → the Principal has a hard time choosing from the right population of Agents the ones that are most suitable for him / her
- Moral hazard → the Principal has a hard time controlling that the Agent will not change his/her behavior after the contract is signed

- In the black markets…
  - Adverse selection → the Buyer has a hard time assessing the properties of the product he is going to buy
  - Moral hazard → the Buyer has a hard time in monitoring the Seller after the purchase happened, e.g. to have the product delivered and functioning as promised

Black markets vs Adverse Selection

- Principal → Buyer ; Agent → Seller
- How does the Buyer choose the right Seller with the right product for him?
  - Sellers surely have no EU Certification for the quality and characteristics of their products
- How to choose the product?
  - Easiest solution: test it!
- Sellers (especially new ones) often provide *trial versions* of their products
- *.. Or give you demonstrations of their functionalities*

Black markets vs Adverse Selection

<video of product functionalities>

Black markets vs Moral Hazard

- Let's assume that the buyer paid an Exploit Kit license to the seller
  - How can the buyer trust the seller in not changing his behavior?
    - E.g. stealing the buyer's infections by dropping his own malware to the machines attacked by the buyer?
- Reputation, Reputation, Reputation. And User History
- There is a very strong **regulatory** mechanism in place
  - Bad users can be reported
  - "Offender lists" are maintained
    - Scammers are put to "public shame"
  - This results in a very strong reputation mechanism

SECONOMICS

TENACE

Market Fairness

- A market only exists when there are sellers that enter the markets and buyer that exchange money for products or services
- Imagine yourself (a criminal) trying to sell your product in a new market
  - Would you really mind scamming people if there is no “punishment” you fear?
  - If you fear punishment, would you spend effort time and money in making a good product if you feel like anybody (e.g. the competition) can just ruin you by telling everybody you are a scammer?
- → the system should be equilibrated:
  - Punishment must be **feared**
  - But also must be perceived as **fair**

Trials: The rules (in short)

- Anybody can report anybody else for trial
- Must include
  - Name and profile of the offender
  - Proof of the fact
- The reporter (accuser) and the reported (defender) enter the trial
- The defender has 24 hours to show up
  - In particularly complicated cases the defender can be given up to 7 days
    - → this decision is taken by the Judge (i.e. administrator)
- An investigation follows:
  - Witnesses are called
  - Evidence of either cases (accuser or defender) is provided
- Administrator takes a decision: Black List or Innocent
- **→ I'll tell you three stories taken directly from the markets**

SECONOMICS

TENACE

(1) The defender does not show up

- **October 2013**
- Accuser reports he has been scammed for 390 US $ by defender
- A moderator ("Arbiter") advices to

  "notify the defender with a personal message [about your report]"
- A third user shows up, reporting that

  "[Contacting the defender is] Useless, he has not been online for a long time"
- Administrator shows up, and gives the defender 48 hours to show up
- Four days later (the 49th hour was Sunday) the adiministrator puts the defender in the black list

(2) The defender loses the trial

- **July 2012**
- Payment of 3000 WMZ not received;
  - defender is given 12 hours to show up
- Defender shows up after 4 hours
  - Brings evidence of payment (very long discussion)
    - Posts logs & screenshots of transaction
- Accuser answers that the payment has never been received
  - He/She accuses the defender to have “blocked” or “intercepted” the payment
  - Witnesses on his side show up to support his claims and trustworthiness
- Admin gives two options
  - 1) Defender must provide final proof of transaction commit
  - 2) Defender and Accuser resolve the case in private
- → after a month of discussion the defendant hasn’t provided conclusive evidence → he ends up “in the Black”

(3) The defender wins the trial

- **October 2012**
- Accuser reports a failure on the defender’s side to close a transaction
- Reports IRC log of their conversation
  - Accuser pays defender while the latter was offline
  - Defender does not acknowledge the payment and does not come back online in a comfortable “time lapse” for the defender
- Defender shows up shortly after, shows that he never cashed anything
- Admin intervenes and asks

  “[Accuser] please do moneyback. To be precise, [defender] do not touch the checks, and most importantly [accuser] get the money back in your wallet.”
- Accuser stops complaining
- Trial is closed and the defender is not “found not guilty”

Sum up

- Both *adverse selection* and *moral hazard* are well addressed
- A few pointers:
  - Markets are strictly regulated, closed to the public
    - Often language restrictions, pull-in mechanisms
  - Offenders / scammers are punished.. After a trial
    - In which they are given a chance to defend themselves
  - Reputation mechanisms
  - Trial versions of products or public demos of product capabilities/ features
  - Pool of vulnerabilities is virtually infinite
- It's actually better than most <<legal markets>>
- Take away: Attackers have a solid infrastructural and economic support from the cybercrime community
  - No reason to believe these markets will cease to exist

The MalwareLab

SECONOMICS

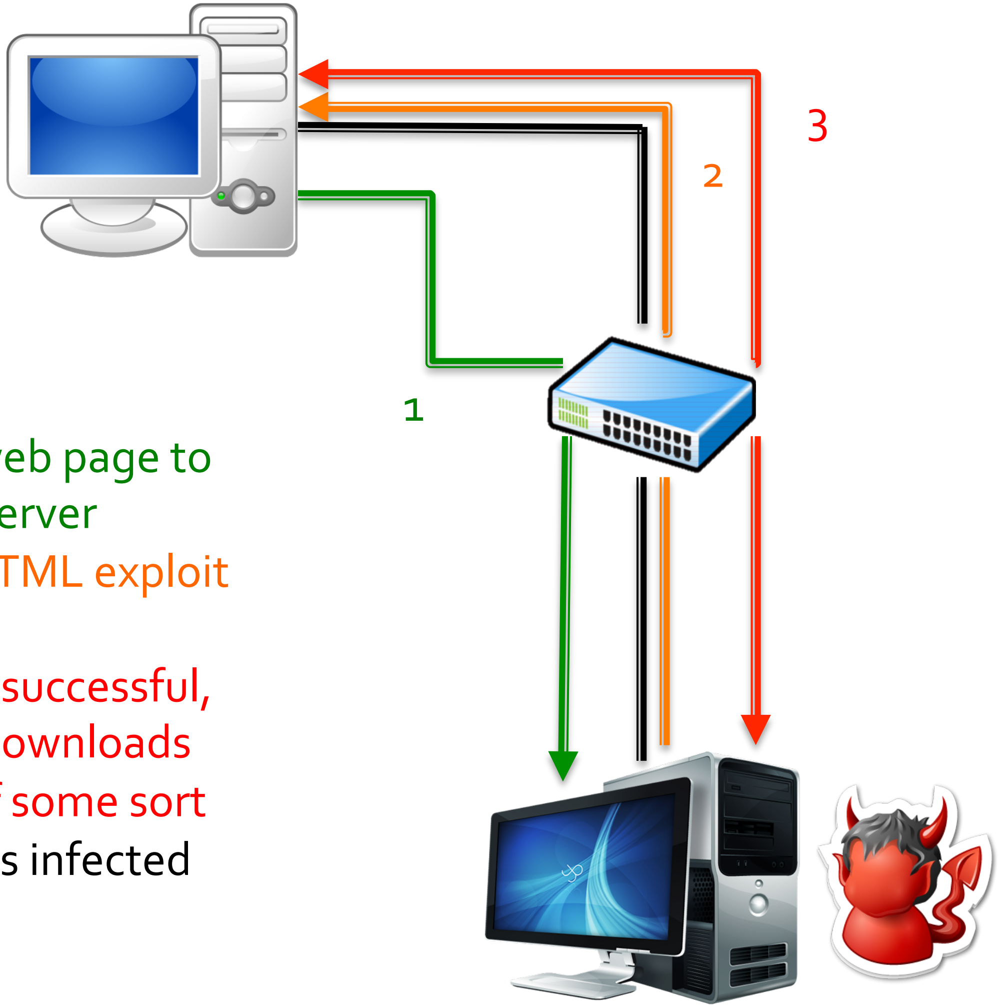
TENACE

- A platform to test malware products from the black markets as "software artifacts"

- Maintained at the University of Trento
  - Developed by collaboration with Vadim Kotov

- In this work we tested 10 exploit kits to answer the following question:
  - *How resilient are Exploit Kits against software updates?*
  - **Goal:** create "***meaningful software configurations that evolve in time and test them against a set of Exploit Kits***"

A reminder: EKITS (simplified) model



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

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

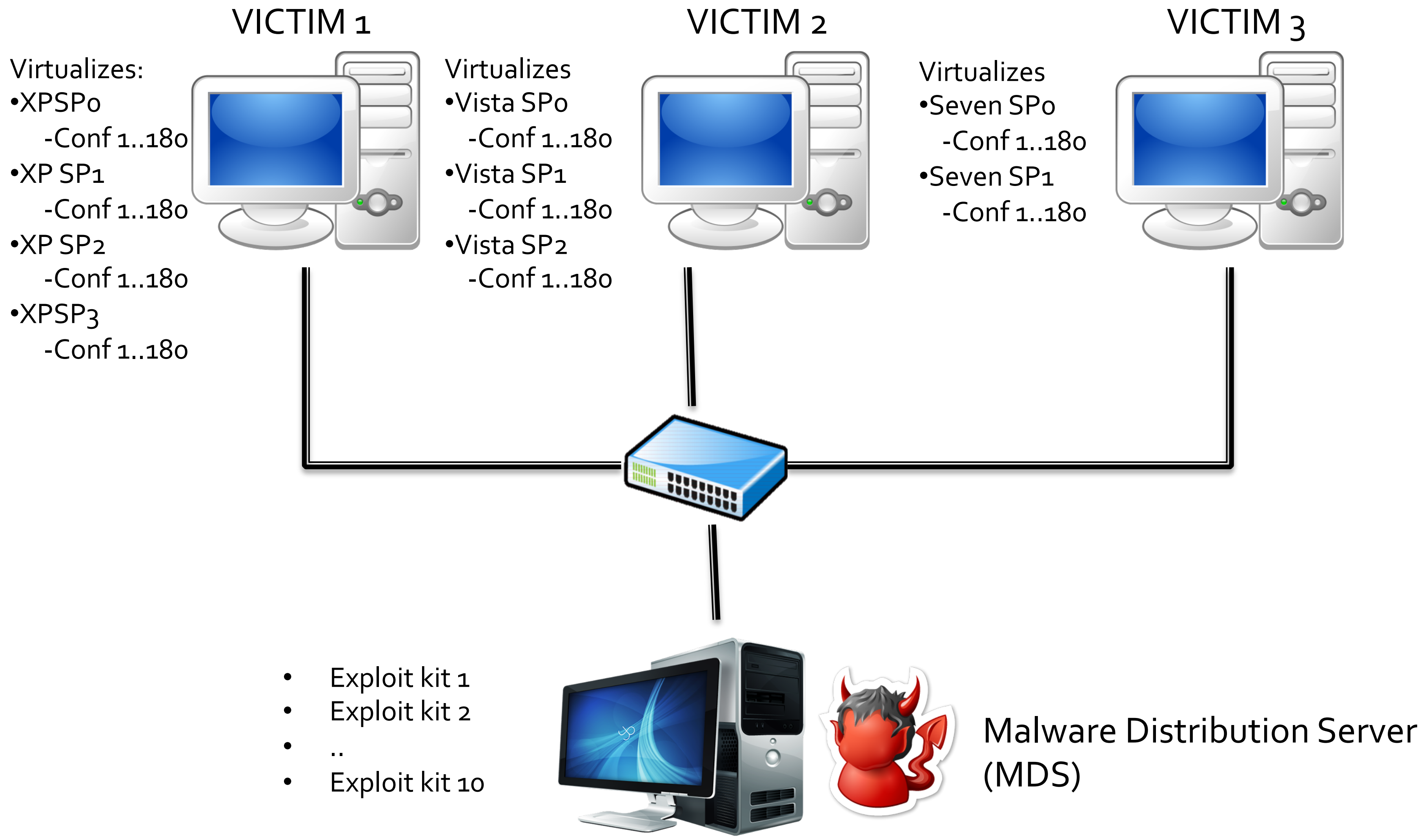
- Exploit kits span from (2007-2011)
  - How we chose the exploit kits
    - Release date
    - Popularity (as reported in industry reports)
    - CrimePack, Eleonore, Bleeding Life, Shaman, …
- Software: most popular one
  - Windows XP, Vista, Seven
    - All service packs are treated like independent 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

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



VICTIM 1

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

VICTIM 2

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

VICTIM 3

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

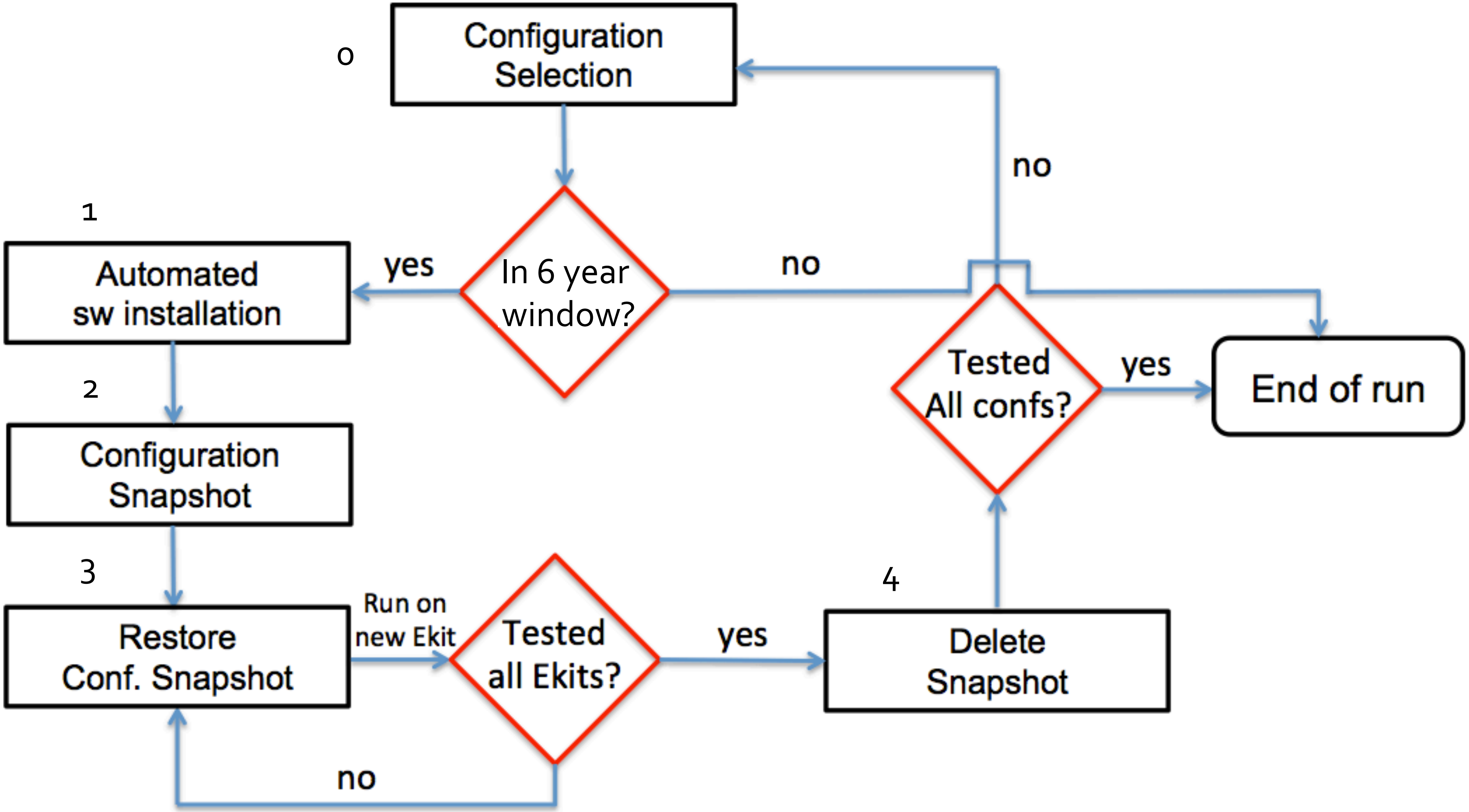
- Exploit kit 1
- Exploit kit 2
- ..
- Exploit kit 10

Malware Distribution Server (MDS)

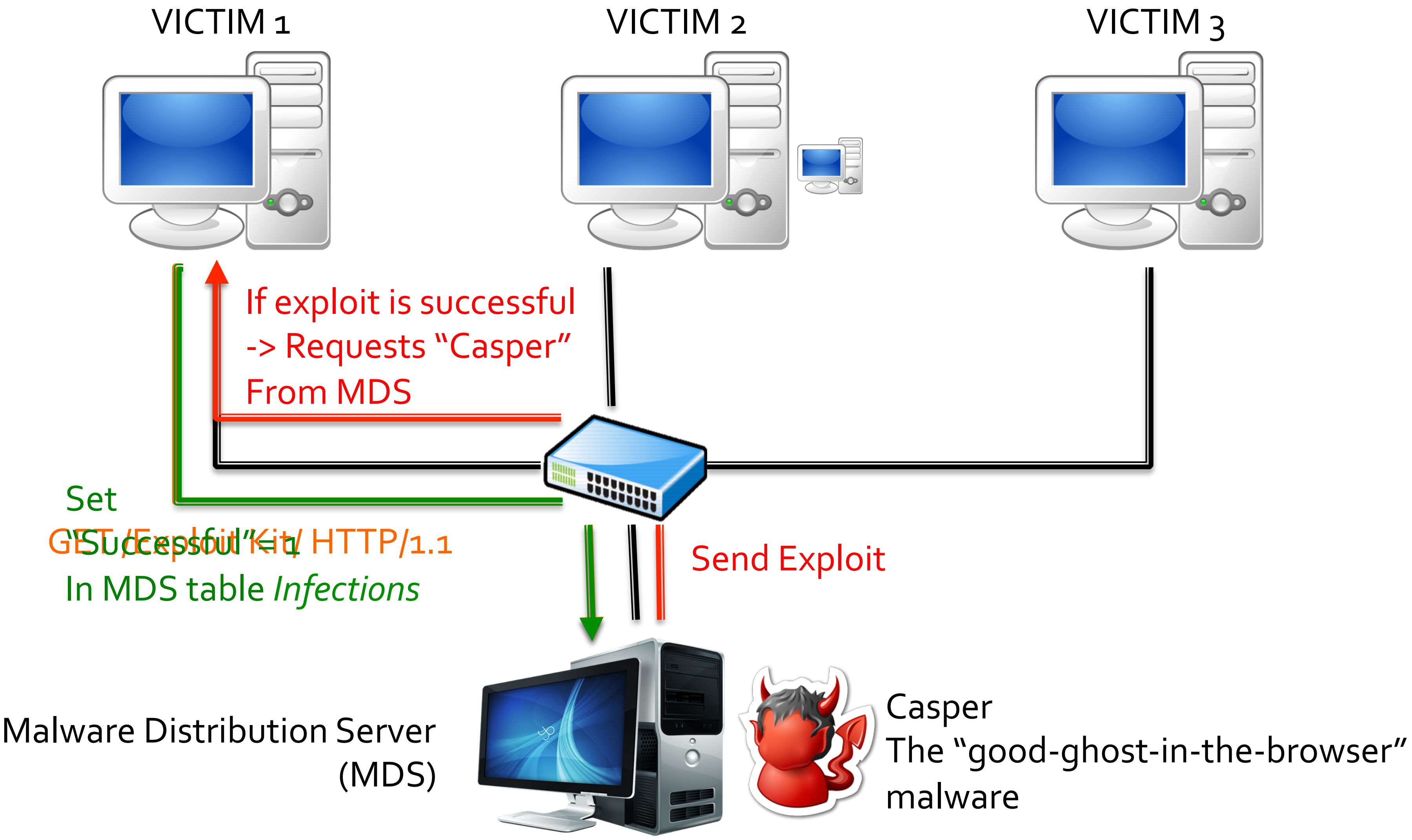
SECONOMICS

TENACE

Overview of the experiment



Assessing exploit successes



If exploit is successful
-> Requests “Casper”
From MDS

Set “Successful”=1
In MDS table *Infections*

GET /Exploit Kit/ HTTP/1.1

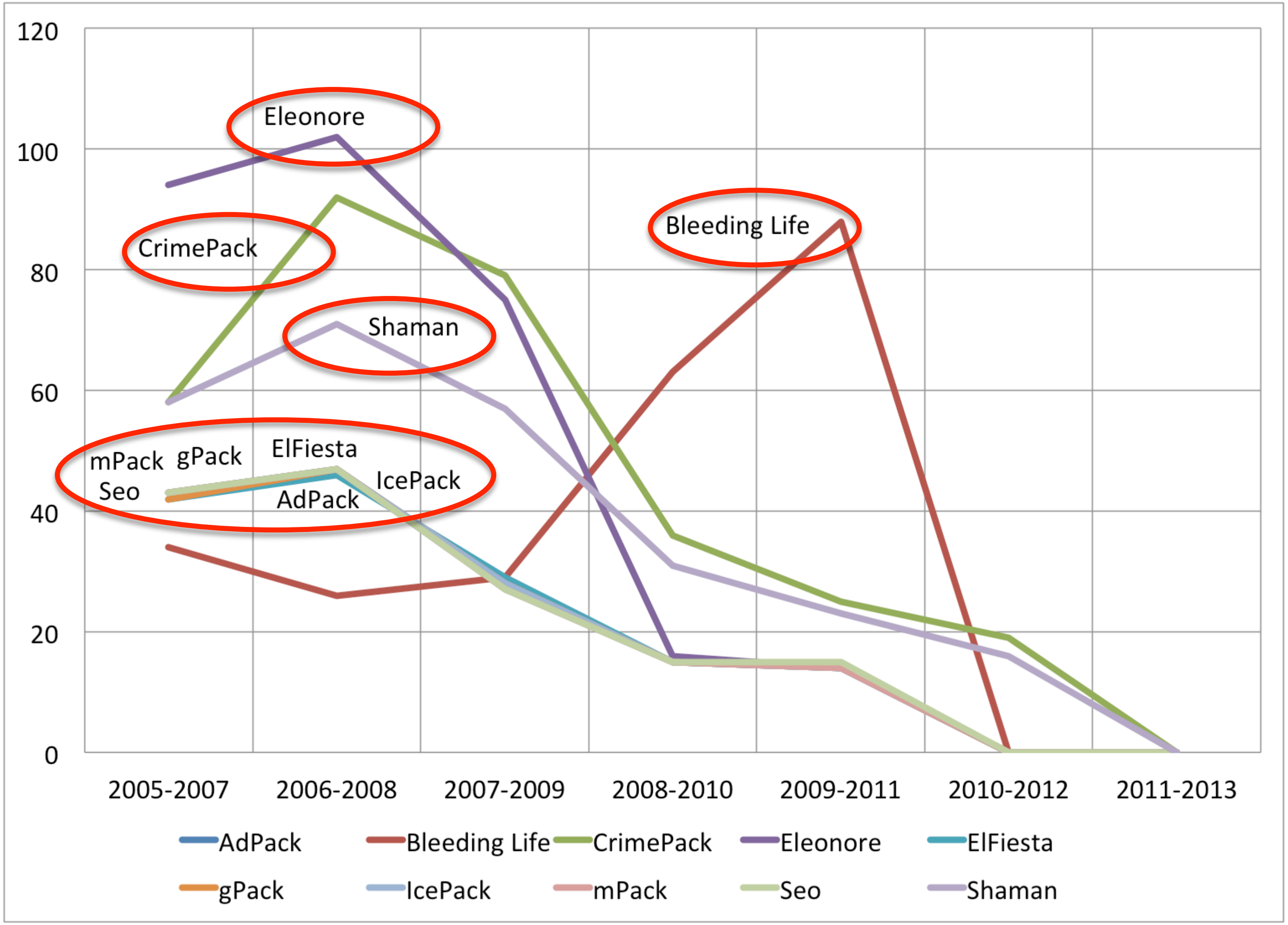
Send Exploit

Malware Distribution Server (MDS)

Casper
The “good-ghost-in-the-browser” malware

SECONOMICS

Results: Infection



Final remarks

- Black markets are well organized, well-functioning markets
  - Feature quality products
  - Address Moral Hazard and Adverse selection properly
- Not all exploits kits are equally good (or bad)
- 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