UNIVERSITÀ DEGLI STUDI
DI TRENTO

SECONOMICS

Some preliminary analysis of the economics of malware kits and traffic brokers

Workshop on "Collaborative Security and Privacy Technologies"

Luca Allodi, Fabio Massacci

25 April 2012, Berlin

Malware Markets

- Initially markets mainly traded goods such as
  - CCNs
  - SSNs
  - Bank accounts
- Initially took place on IRC channels
  - No proper moderation
  - No reputation system
  - It was a market for "Lemons"[1]
- No ROIs → This paradigm failed

1. C. Herley and D. Florencio. Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy. Economics of Information Security and Privacy, 2010.

New Malware Markets

- Forums/e-commerce sites
- New features
  - Reputation Systems
  - Brokerage of tools
  - Infrastructure of services
    - Additional services to support the tools
  - "Language restricted" markets
- Feature the characteristics of a typical growing market

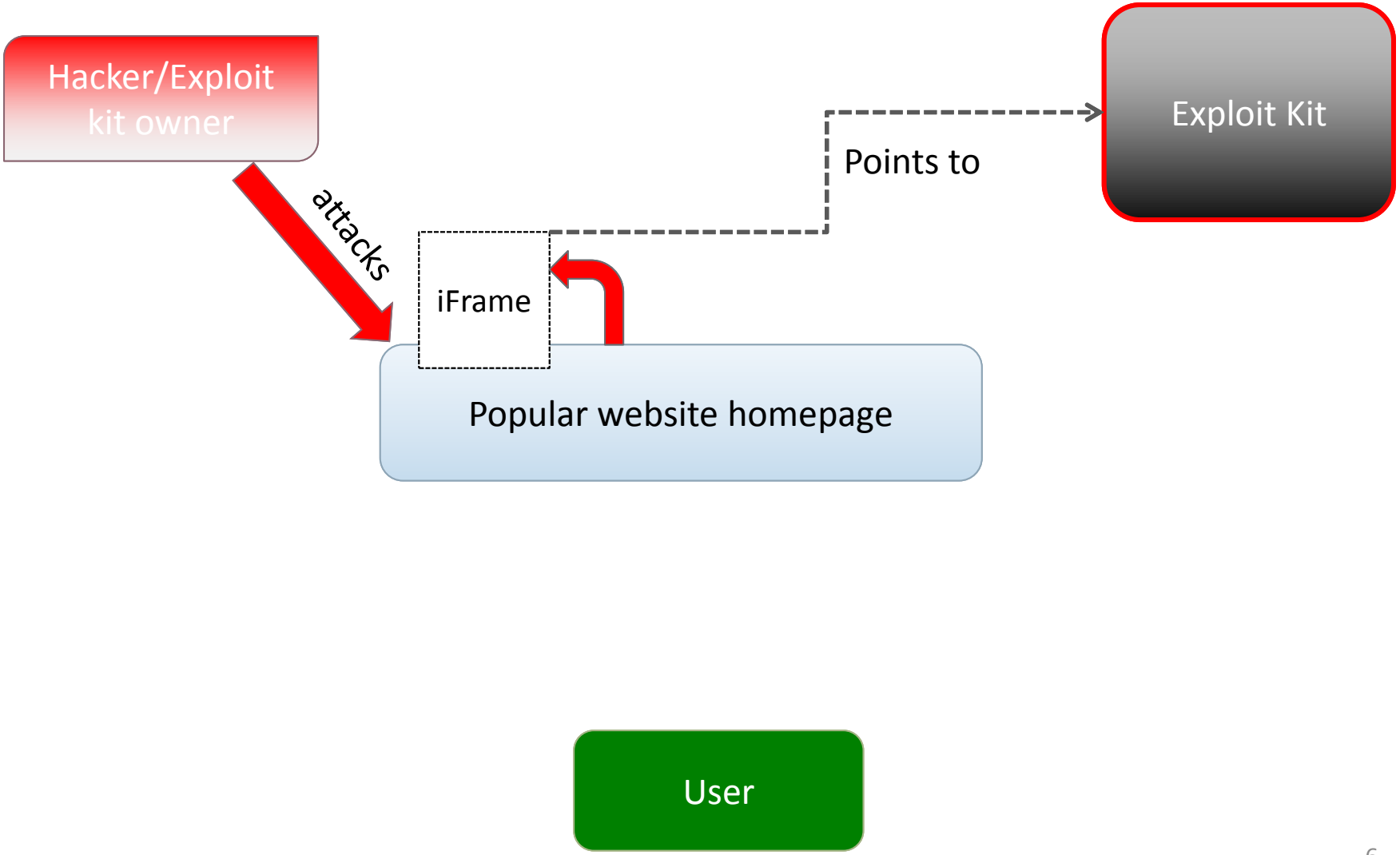
Who the attackers were, and are

- ’90s: hackers were security enthusiasts with high technical competence
- ’00s: hacker was anybody that could run an automated tool
- ‘10s: hackers are economic agents that look toward ROIs
  - Automation tools are not enough now
  - Trade of infrastructure
    - Exploit Kits
    - Traffic Brokers

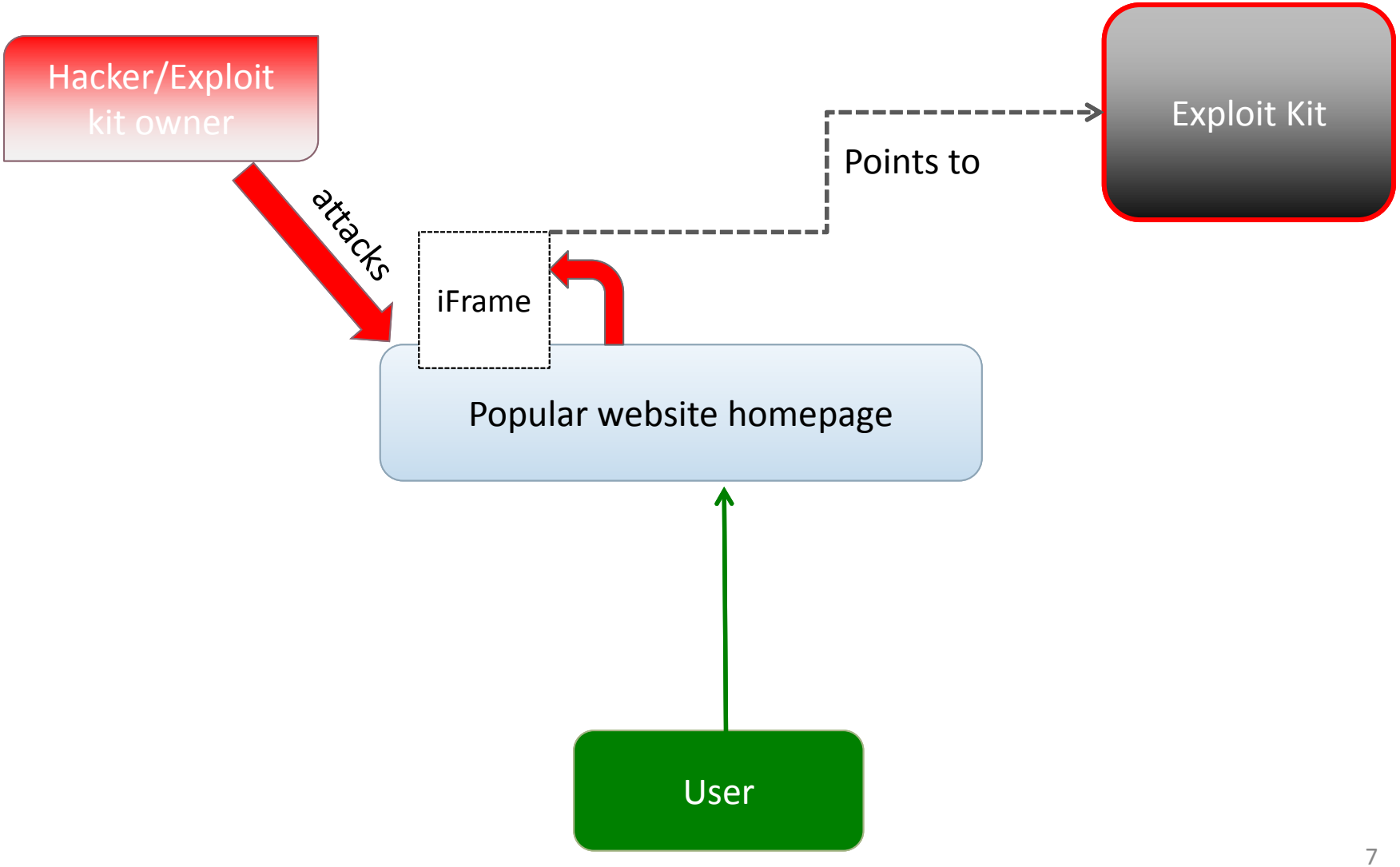
Exploit Kits and Traffic Brokers

- Exploit kits are web applications deployed on some server
  - MySQL back-end
  - When the user connects to its `exploit.php' page
    - Exploit kit test victim's configuration for known vulnerabilities -> exploit
    - Shellcode usually initiate download of some malware
- Problem
  - ➢ The attackers needs the user to explicitly make a GET request toward `exploit.php'
- Solution
  - ➢ Buy connections from Traffic Brokers

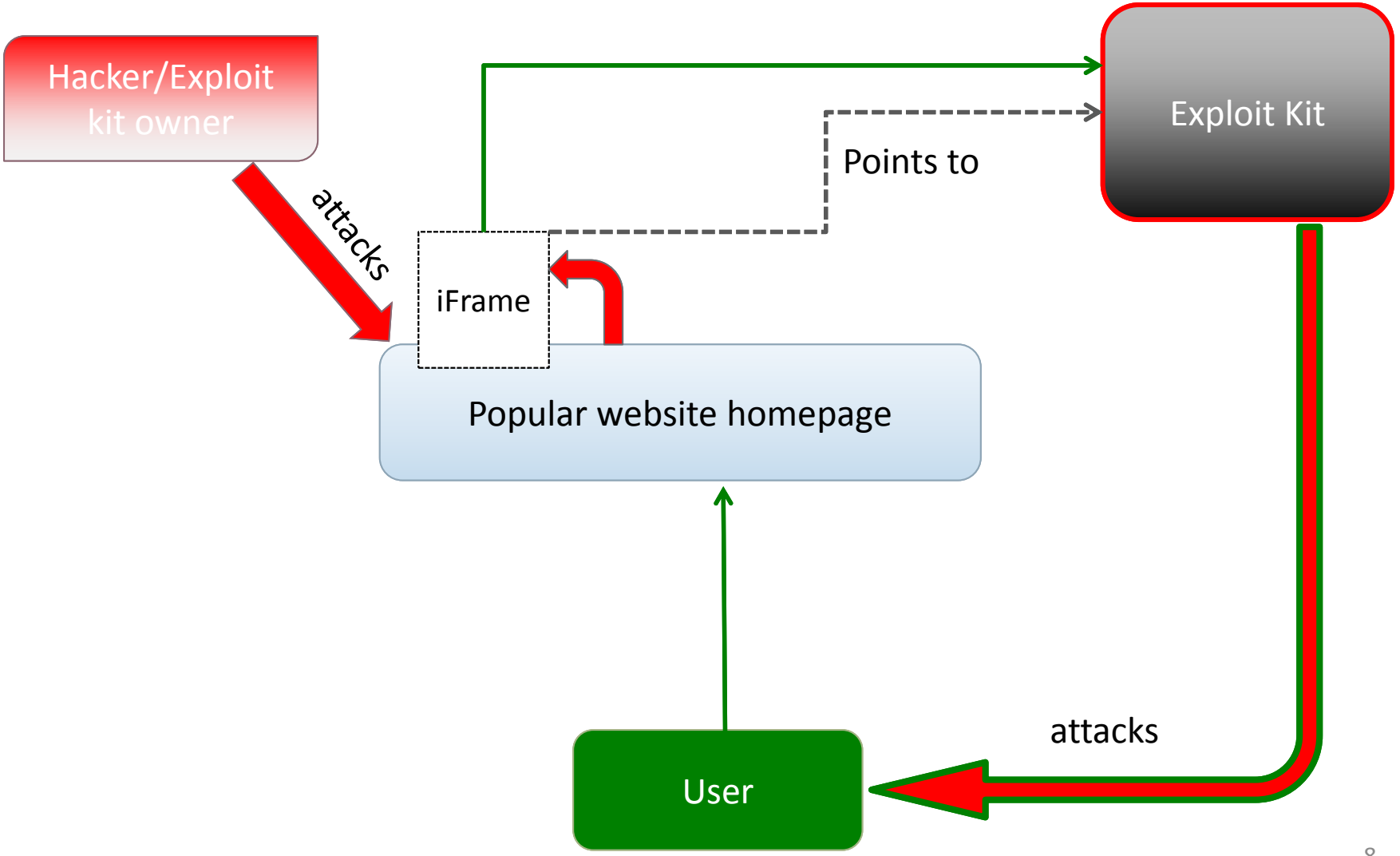
How Exploit Kits work



How Exploit Kits work



How Exploit Kits work



How Exploit Kits are sold

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%

Install rates
Zeus malware: 50-60%
Loader: 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.

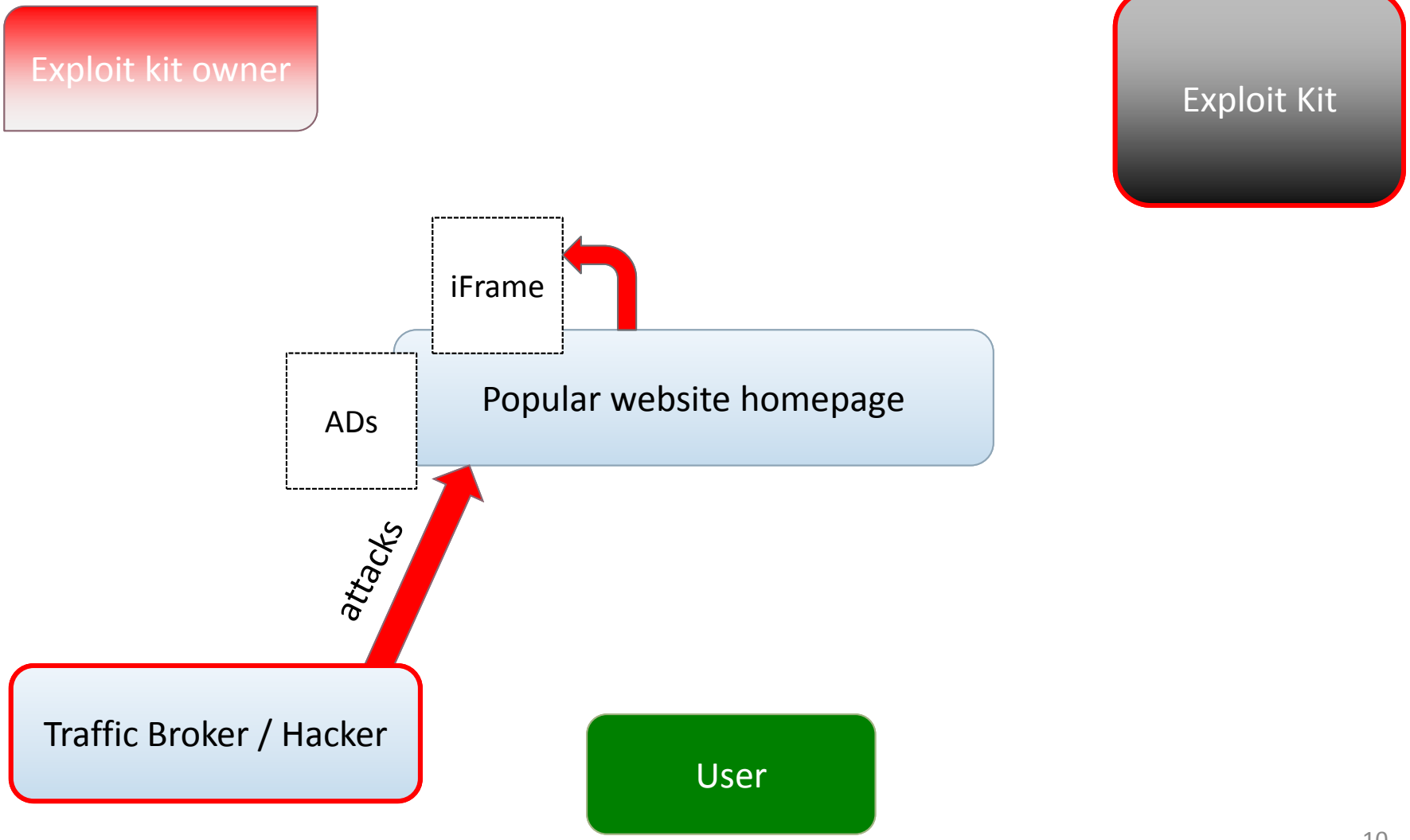
Vendor's contacts
Working hours:
- Monday-Saturday
- 7am to 5pm (Moscow time)

23.03.2011, 19:44

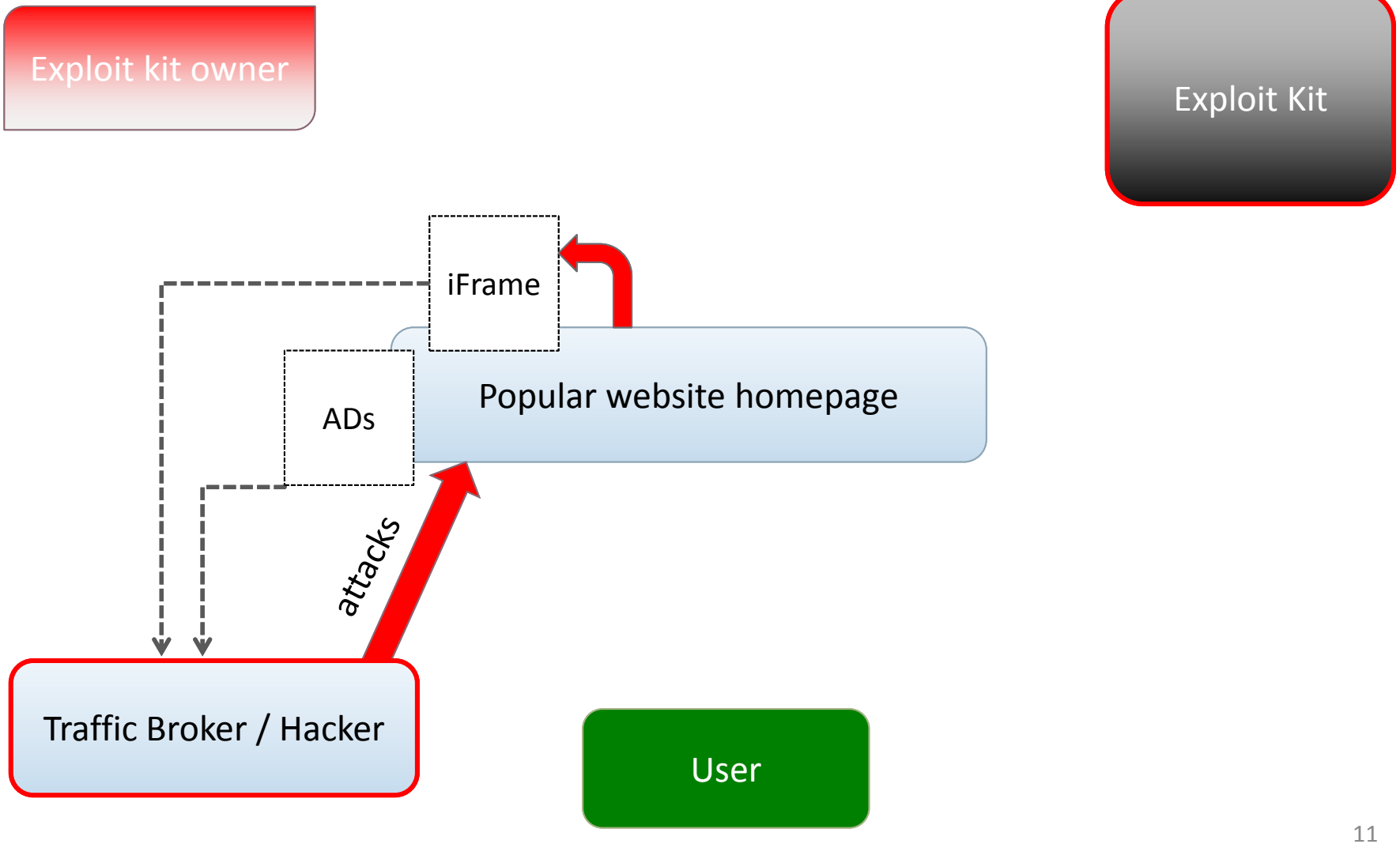
Апдейт до версии "***Eleonore Exp v1.6.5***"

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

How traffic redirection works



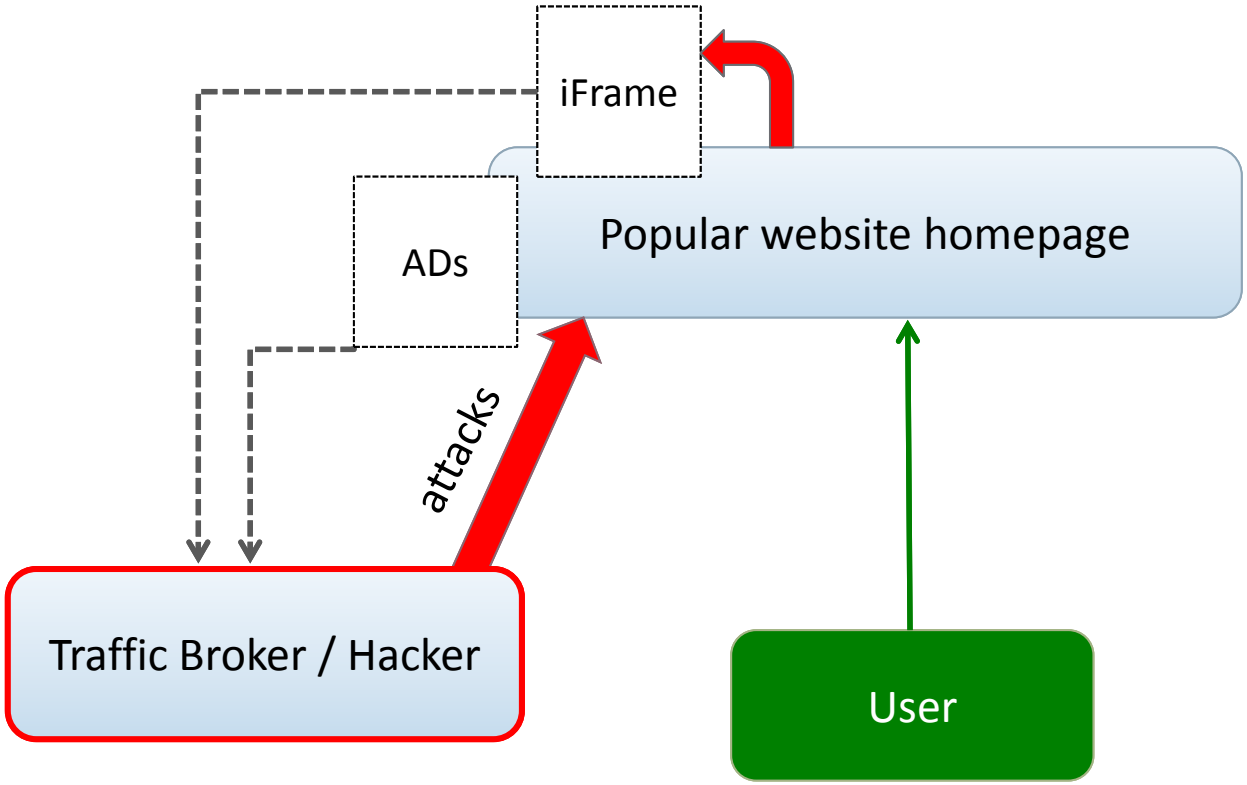
How traffic redirection works



How traffic redirection works

Exploit kit owner

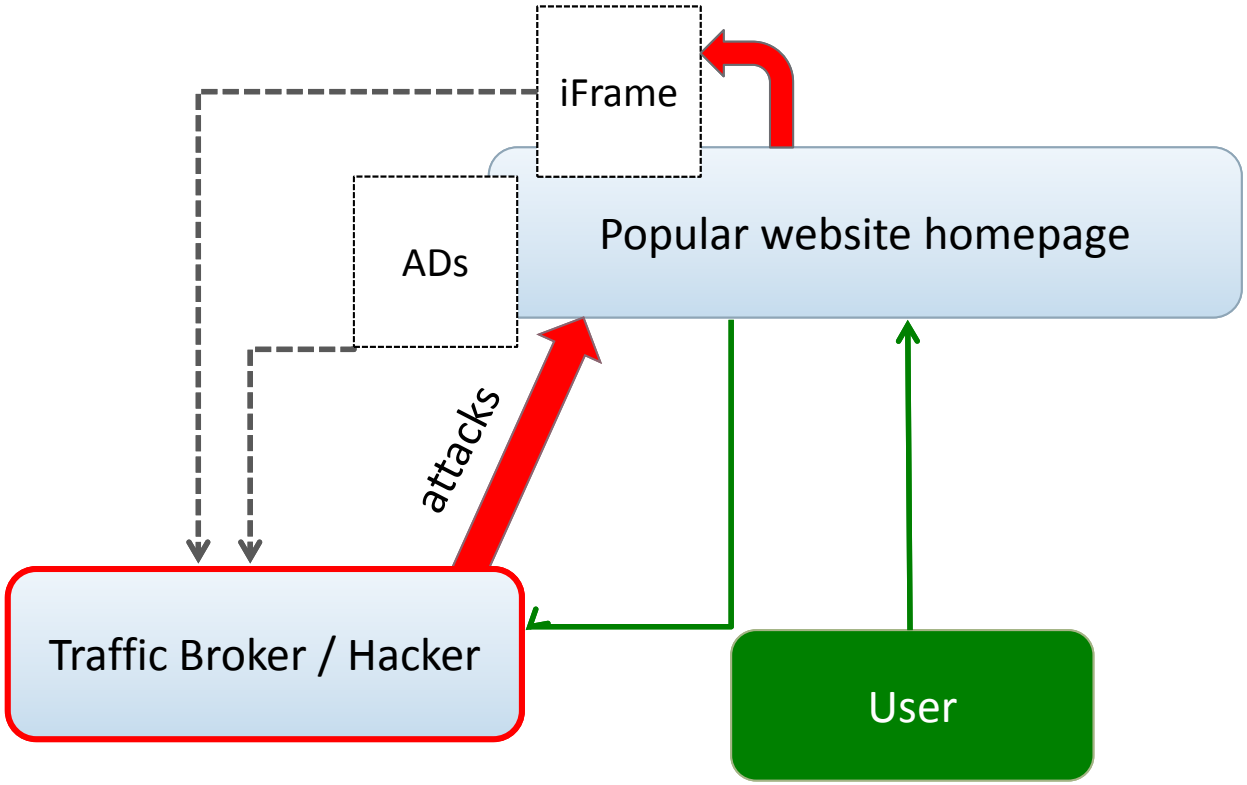
Exploit Kit



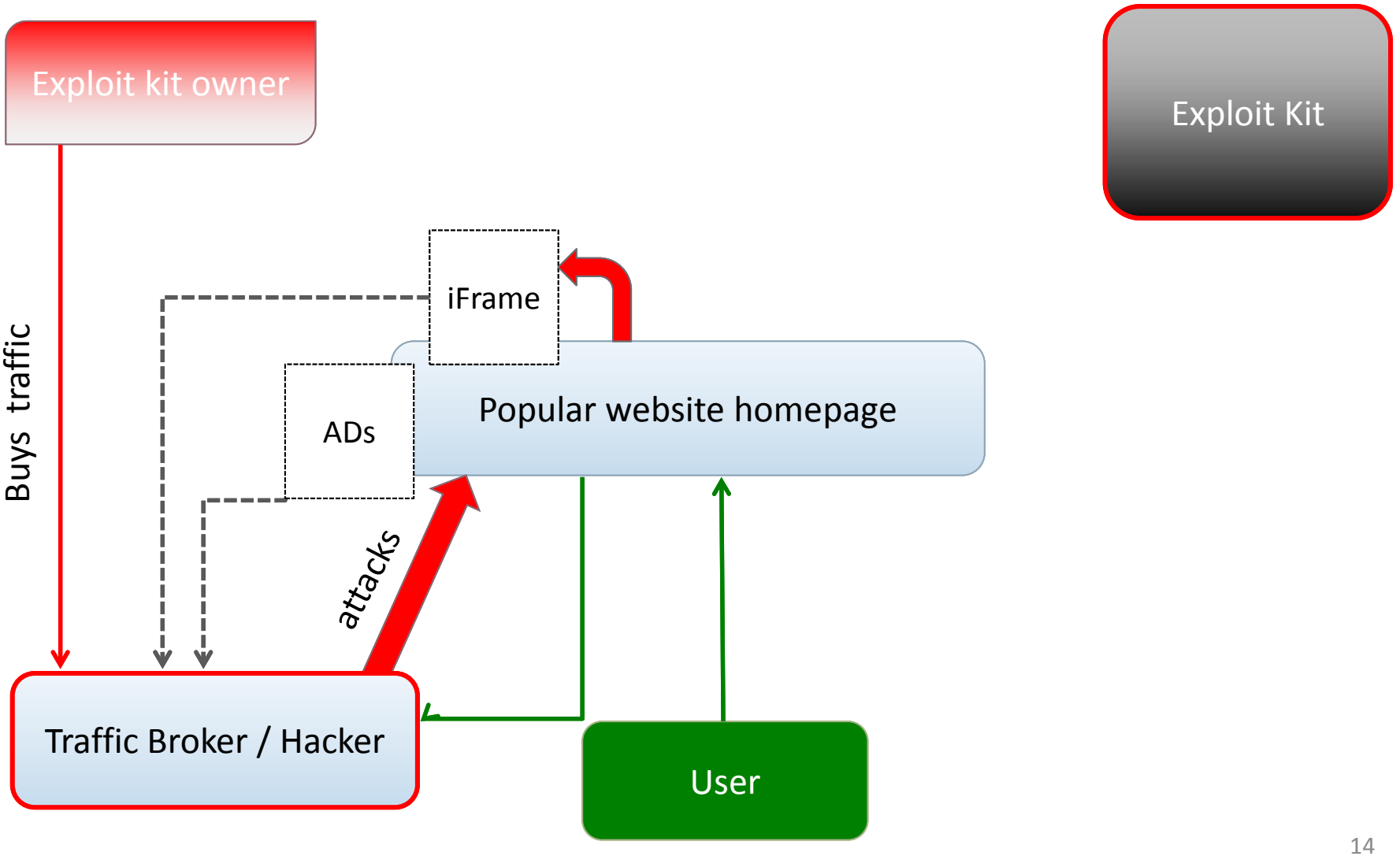
How traffic redirection works

Exploit kit owner

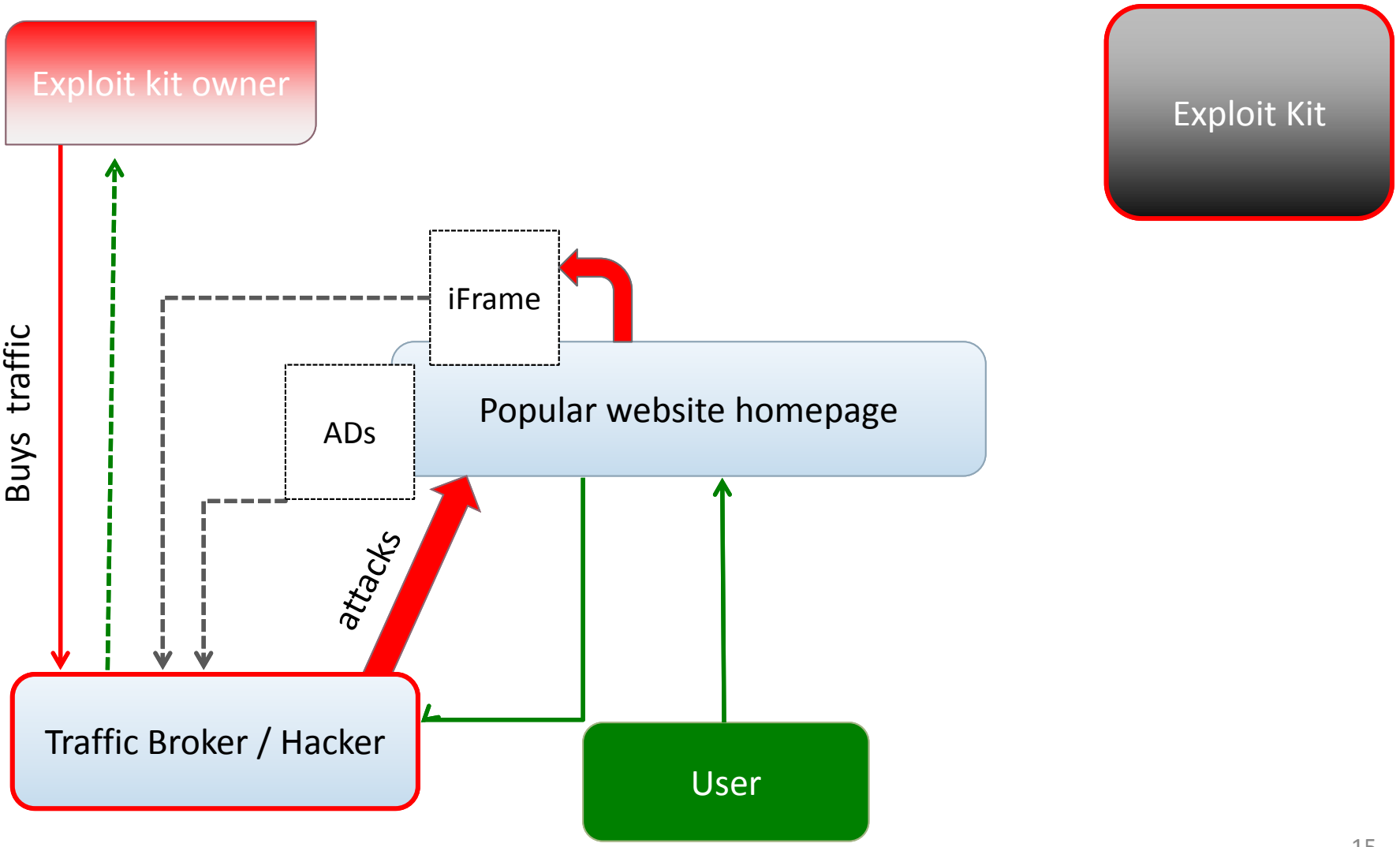
Exploit Kit



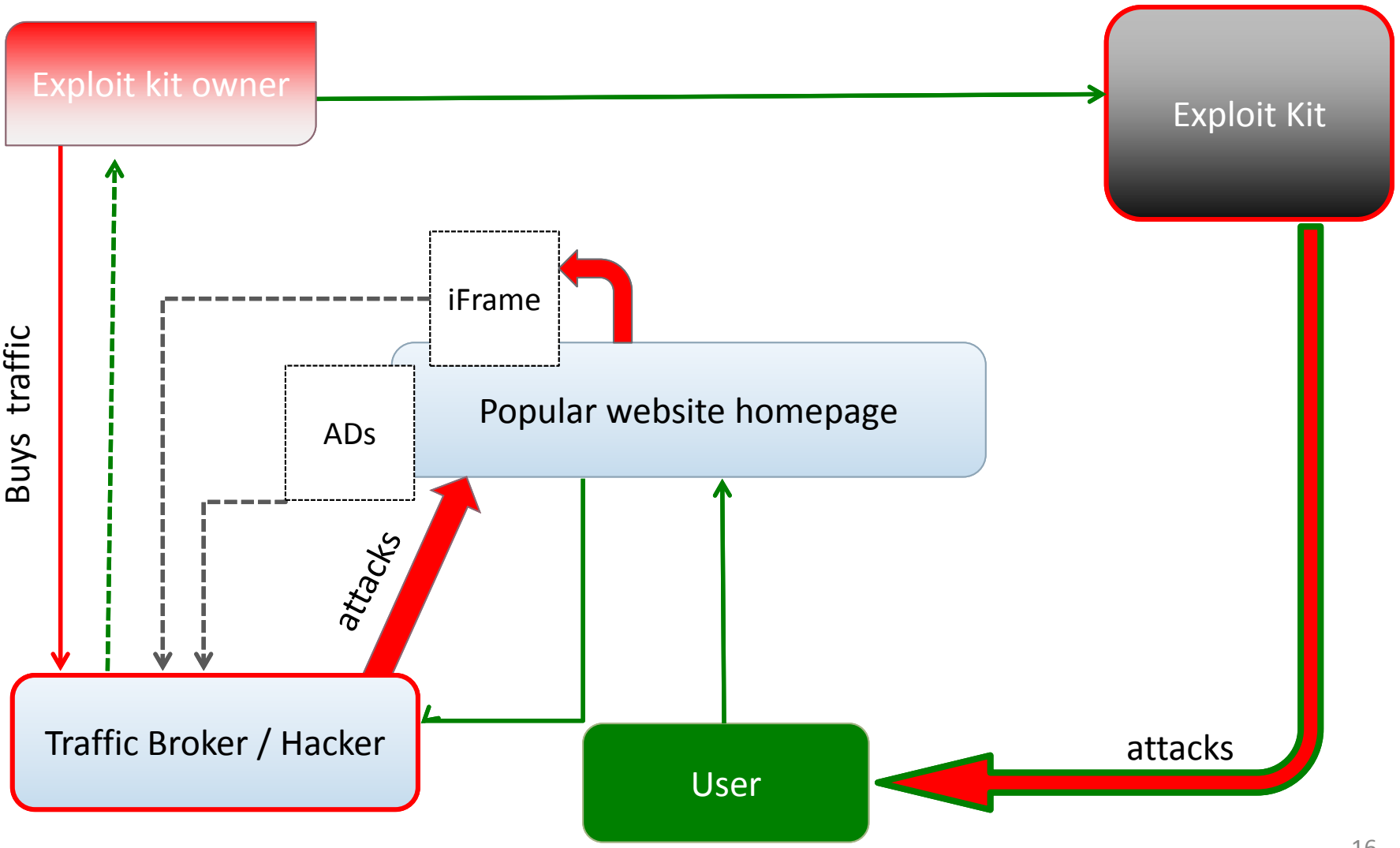
How traffic redirection works



How traffic redirection works

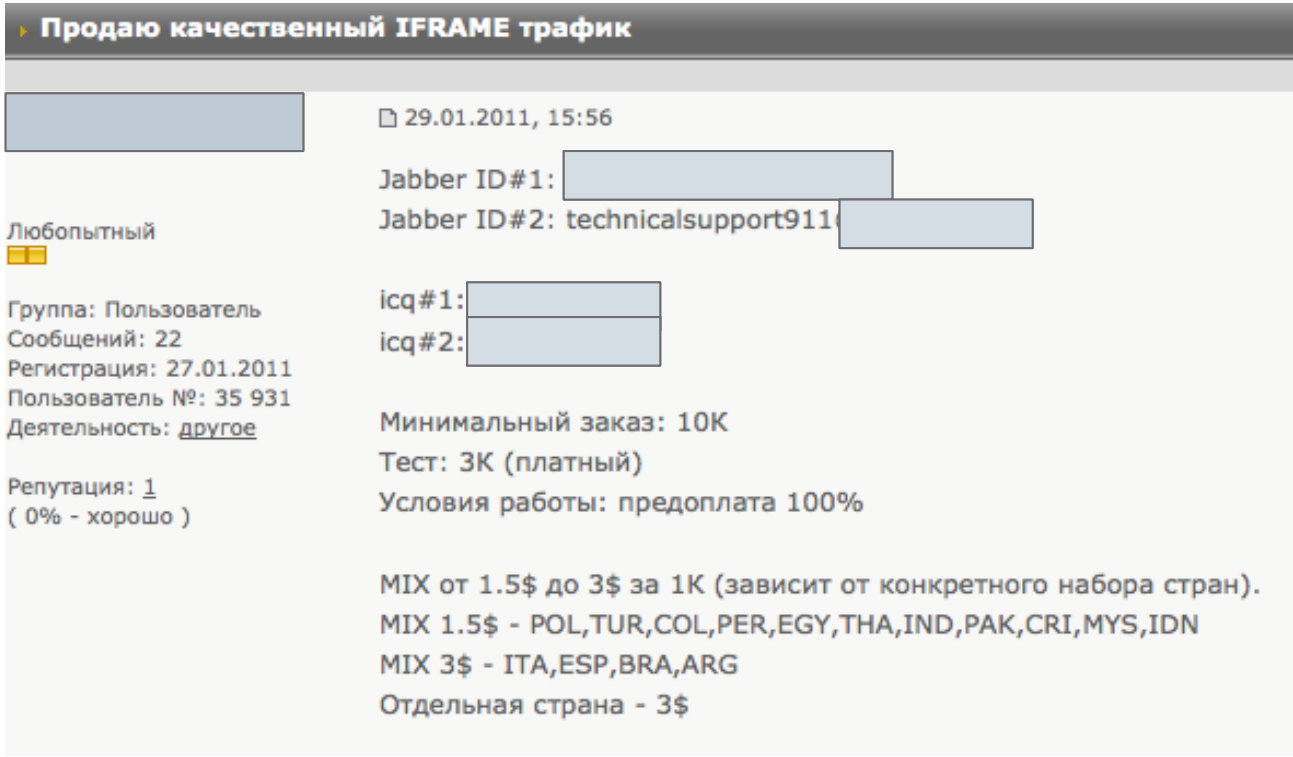


How traffic redirection works



How traffic is sold

- 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



Some math

- Cyber crook wants to build a 1 million bots botnet

Action	Economic effort (1st year)
Number of needed connections	5×10^6
Buy Traffic (assuming 2USD/1k)	10.000 USD
Updates (assume 2/yr)	~ 200 USD
Total	**~ 12.400 USD – 12.500 USD**
Breakeven ROI/BOT	**~ 0.01 USD**

Thanks!

Any questions?