



UNIVERSITÀ DEGLI STUDI
DI TRENTO



A first analysis of the markets of cyber attacks

Università degli Studi di Trento

Luca Allodi, Fabio Massacci

14 may 2012, Trento

```
* Paypal Verified Account Prices:
1 Paypal verified without balance==30$
1 Paypal verified with 1000$ balance ==50$
BankLogins Prices:
BALANCE IN CHASE .....70K TO 155K =====160$
BALANCE IN WASHOVIA.....24K TO 80K=====80$
BALANCE IN BOA.....75K TO 450K=====300$
BALANCE IN CREDIT UNION.....ANY AMOUNT=====300$
BALANCE IN HALIFAX.....ANY AMOUNT=====300$
BALANCE IN COMPASS.....ANY AMOUNT=====300$
BALANCE IN WELSFARGO.....ANY AMOUNT=====300$
BALANCE IN BARCLAYS.....80K TO 100K=====400$
BALANCE IN ABBEY.....82K =====700$
BALANCE IN HSBC.....50K=====350$
```

- 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.

* Picture taken with permission from Guarnieri's Security Summit 2010 presentation



New Malware Markets



Xio



Вишневый сад
■■■■■

Группа: Пользователь
Сообщений: 130
Регистрация: 24.03.2011
Пользователь №: 36 723
Деятельность: вирусология

Репутация: 12
(1% - хорошо)

❤ 16.01.2012, 15:51

В связи с появлением дополнительных ресурсов открывается новый набор.
Партнерки, крупные клиенты, клиенты с ценным траффом вам ко мне.

Квота : 5 мест. (может быть и меньше, в зависимости от масштаба клиентов)

Intro: Можно сказать что связка прошла успешное испытание временем, доказала свою конкурентноспособность и право на существование.

Я уверен что она придется по вкусу многим. Добро пожаловать в проект **Sakura!** 😊

Текущая версия 1.1

В связку на данный момент входят:

- Java Rhino
- Java Obe
- Pdf Libtiff

Цена:

- 2000\$/месяц при потоках <100к траффика в сутки. При больших потоках цена обговаривается отдельно.

- За 30% траффа US,CA,UK,AU при потоках >50к сутки.

Связка предоставляется бесплатно! Вы не покупаете лицензию.

- Brokerage of **tools**
- Infrastructure of **service**
- Reputation Systems
- “Language restricted” markets



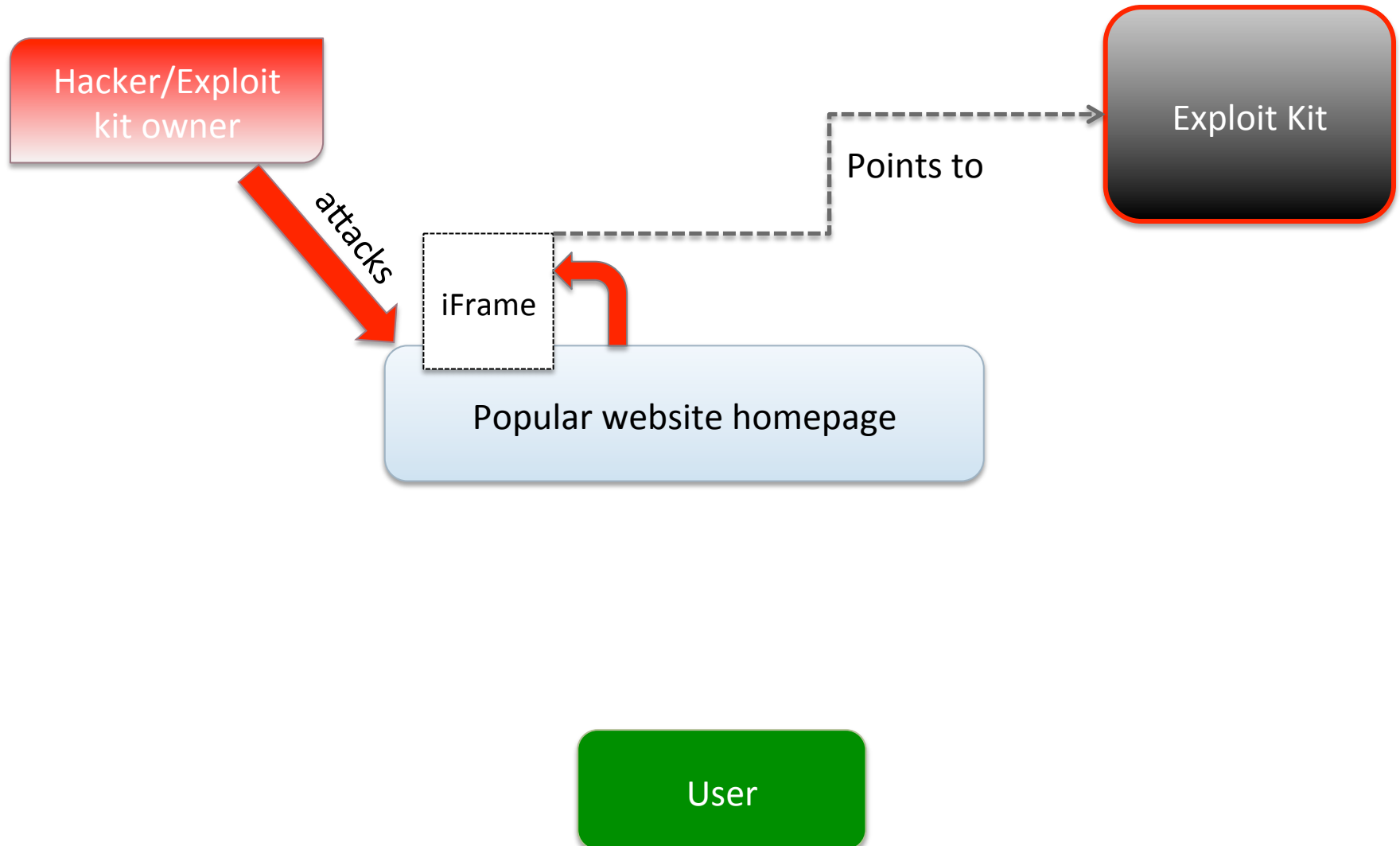
Who the attackers were, and are



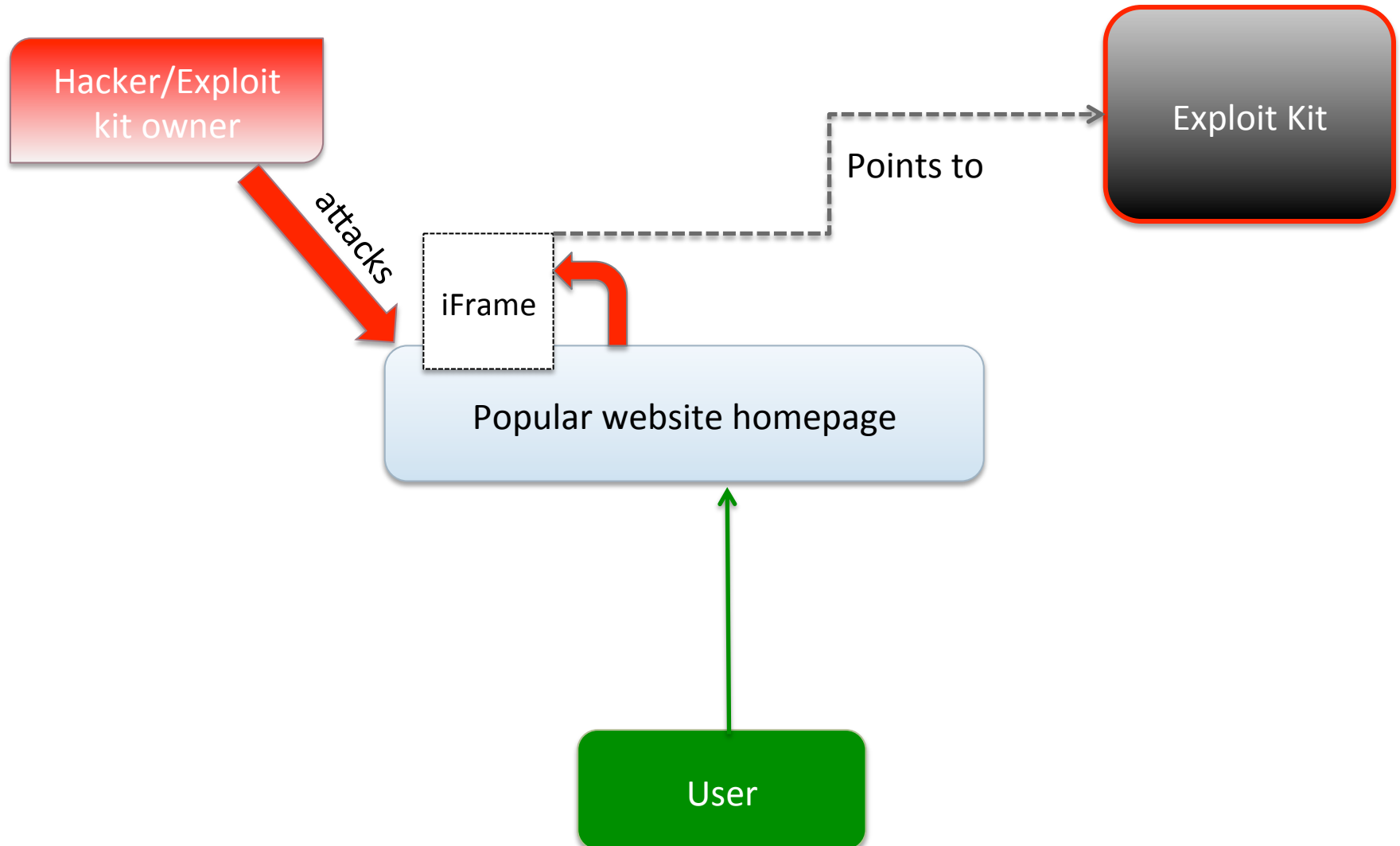
- '90s: hackers were security enthusiasts with high technical competence
- '00s: hacker was anybody that could run an automated tool
- '10s: hackers are **economic agents** that look toward ROIs
 - Automation tools are not enough now
 - **Trade of infrastructure**
 - Exploit Kits
 - Traffic Brokers

- Exploit kits 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

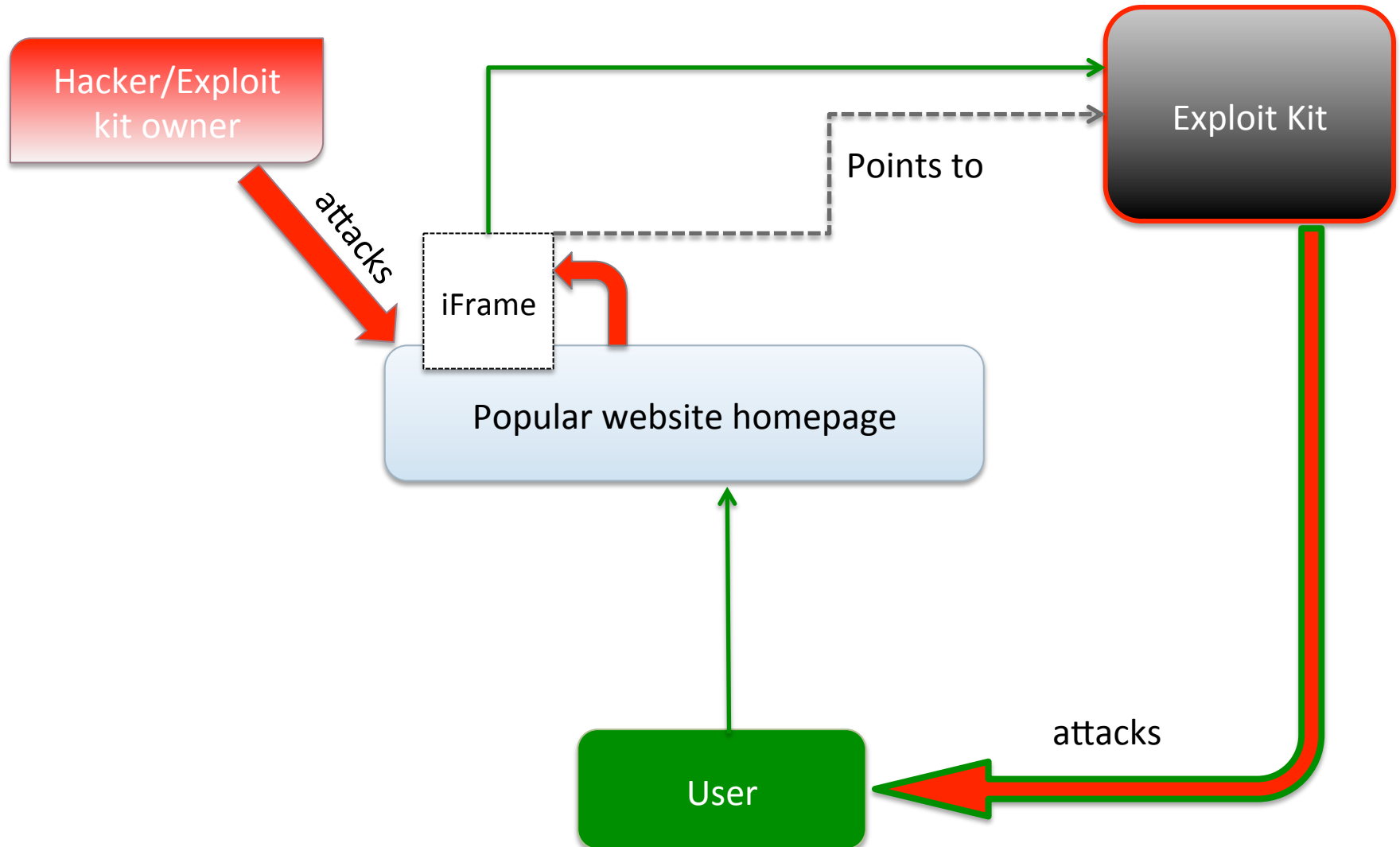
How Exploit Kits work



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 трафика.

* 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 .

Связь:

> ICQ: 9000001

> Jabber: Exmanoize@xmpp.jp

Рабочий график:

> понедельник - суббота

> с 7 до 17 по мск.

Latest prices

Additional services

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

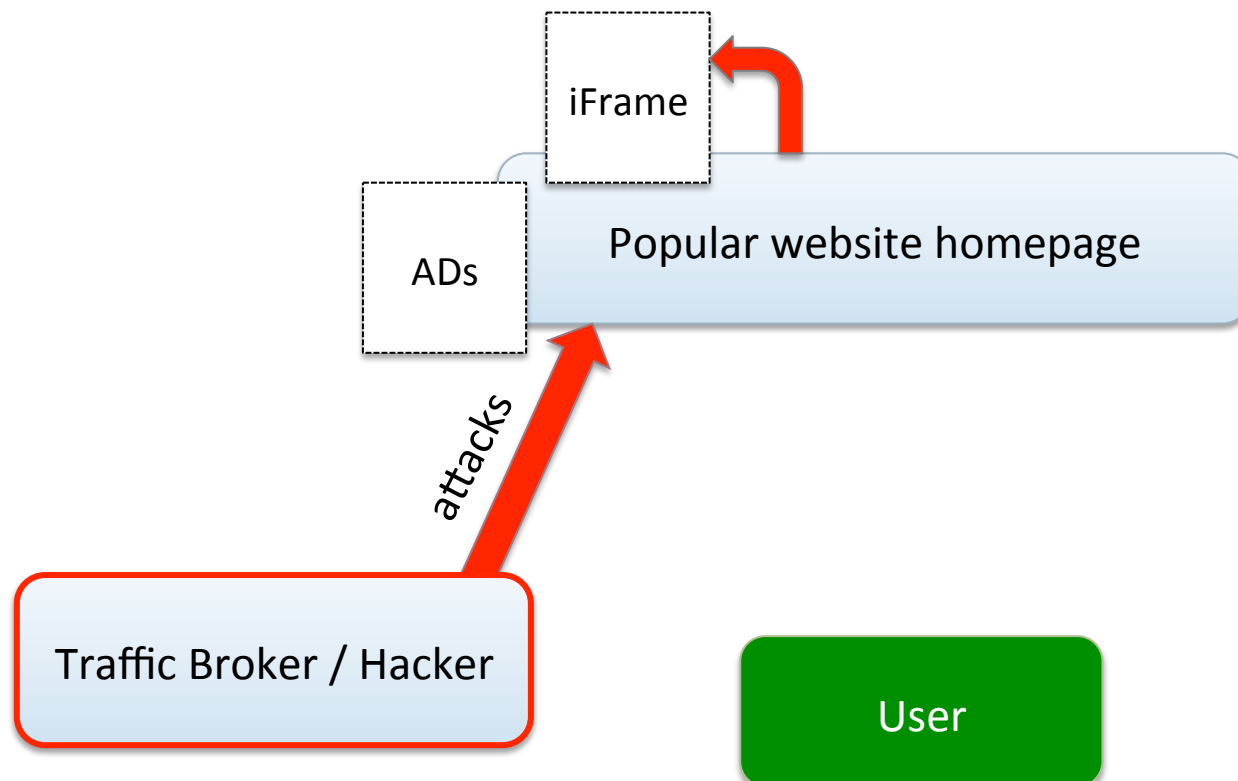


How traffic redirection works



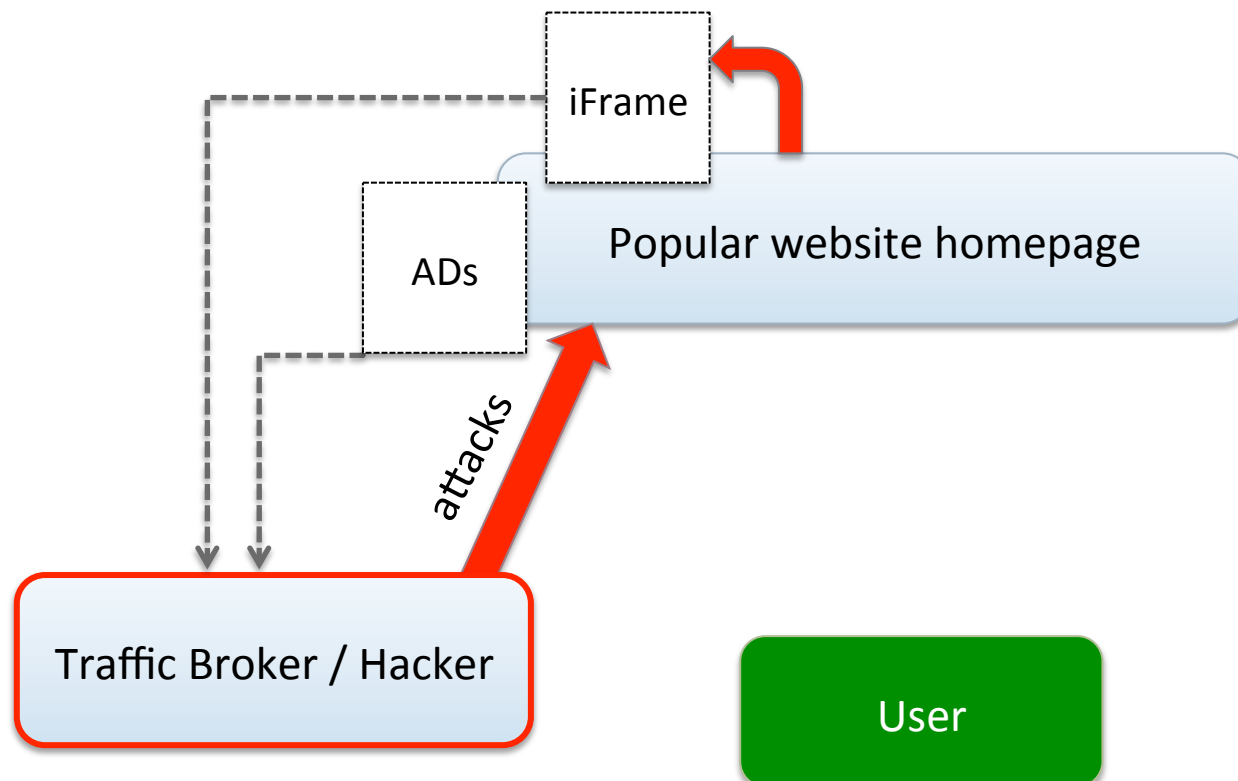
Exploit kit owner

Exploit Kit



Exploit kit owner

Exploit Kit



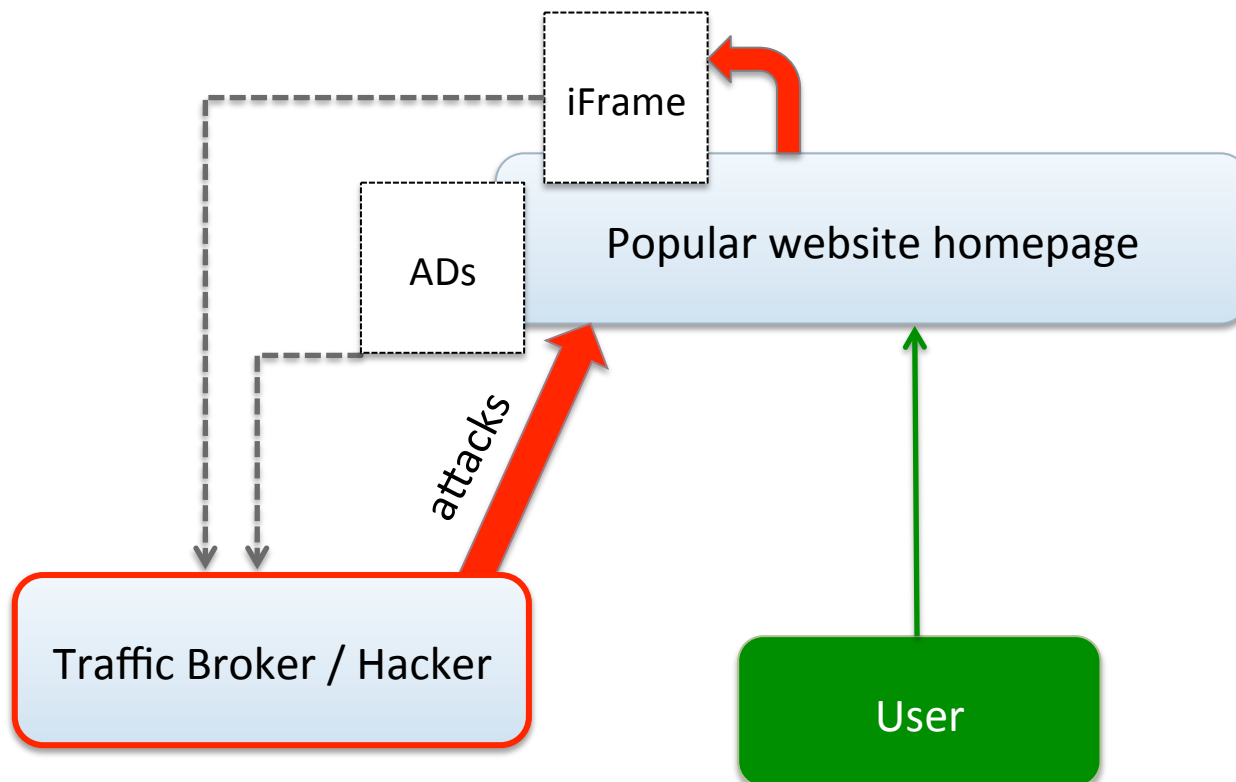


How traffic redirection works



Exploit kit owner

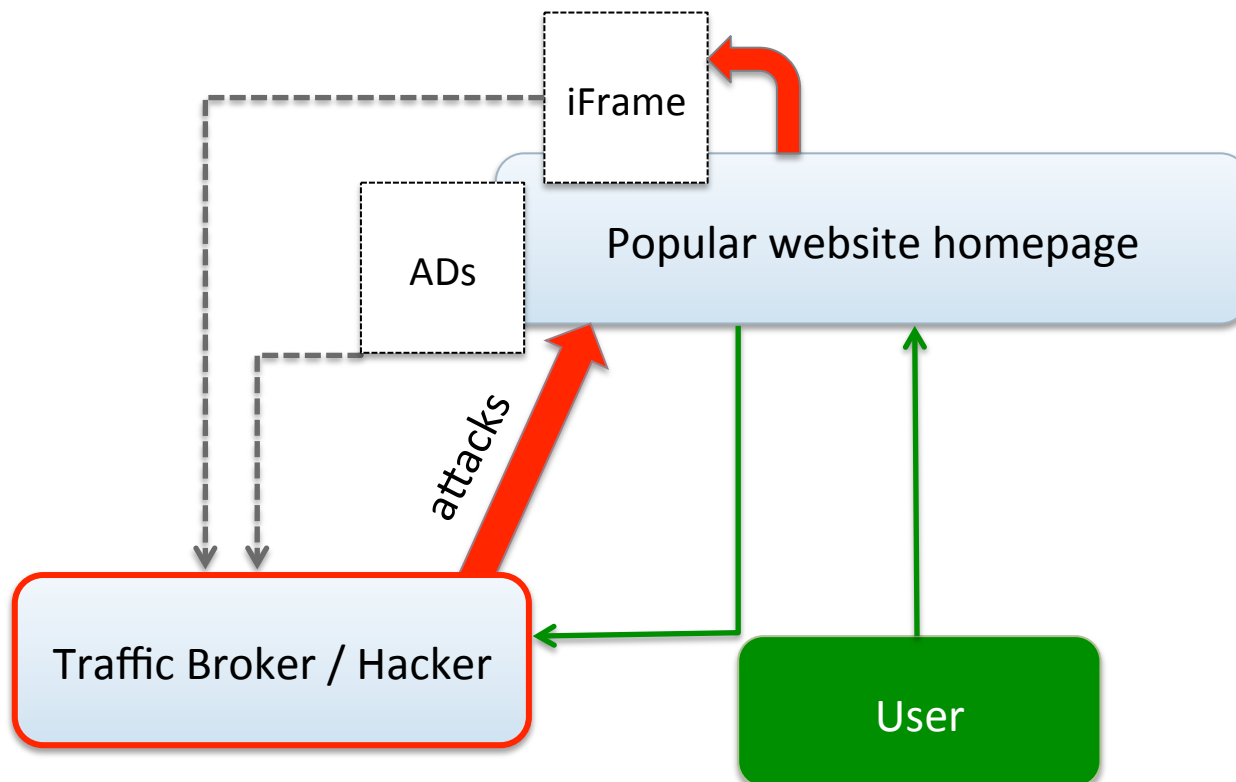
Exploit Kit

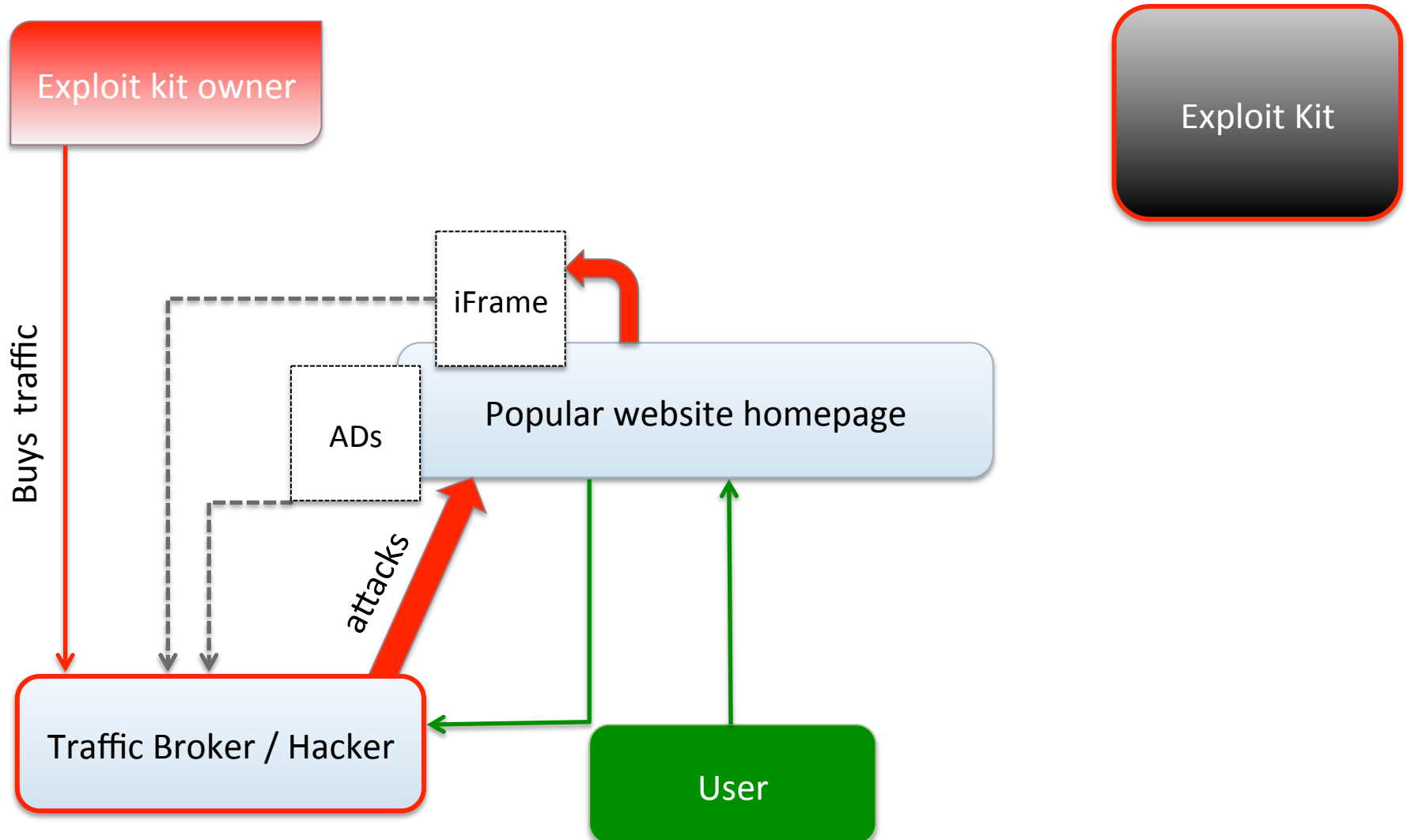


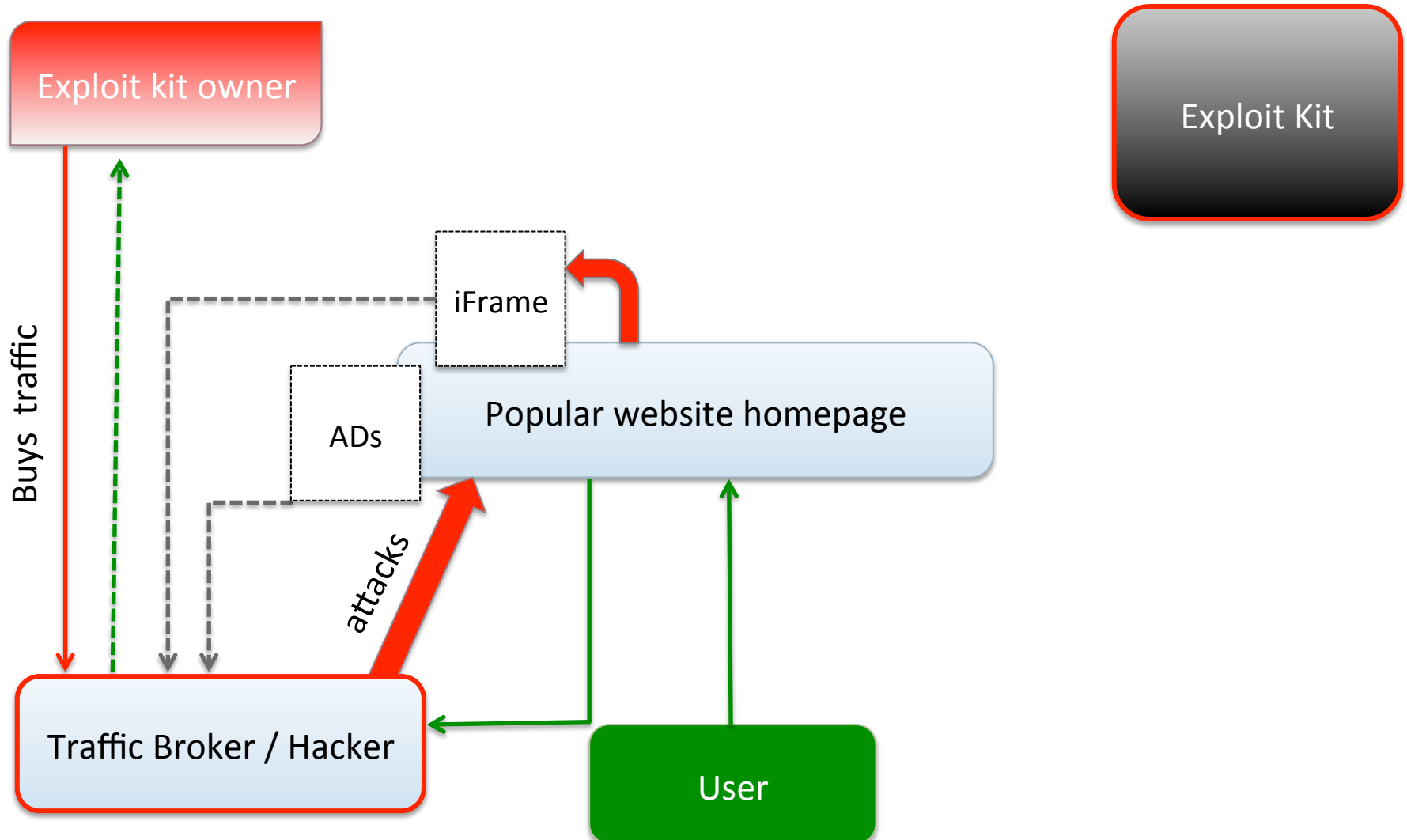
How traffic redirection works

Exploit kit owner

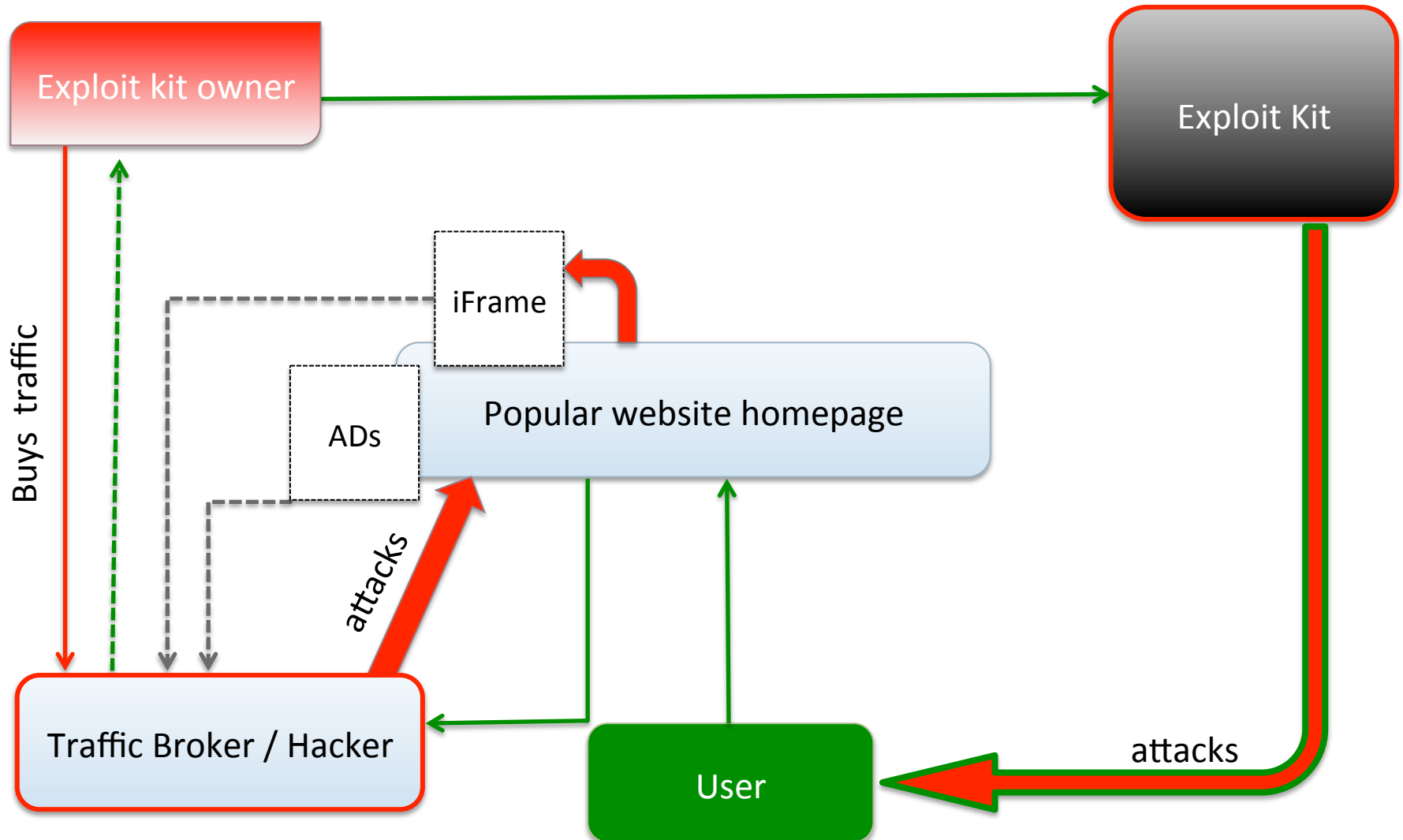
Exploit Kit







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

► Продаю качественный IFRAME трафик

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\$

BUY TRAFFIC	
SELL TRAFFIC	
USER GUIDE	
REGISTER	

BIG TRAFFIC. BIG PROFIT. THINK BIG!

SKIMMED TRAFFIC \$2.00 PER 1K	MOBILE TRAFFIC \$3.32 PER 1K	POPUNDER TRAFFIC \$1.25 PER 1K
---	--	--

GET UP TO **15%** OFF BIG ORDERS

Cyber crook wants to build a 1 million bots botnet

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



Thanks!



Any questions?

