vb 2011
BARCELONA
5-7 October 2011

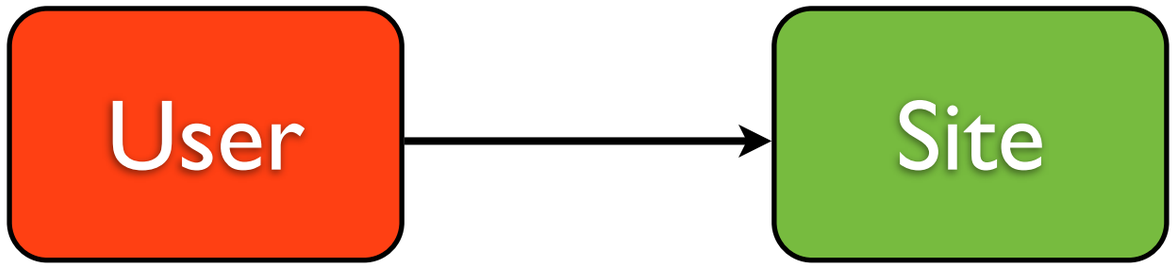
Using Traffic Direction Systems to simplify fraud... and complicate investigations!

Maxim Goncharov

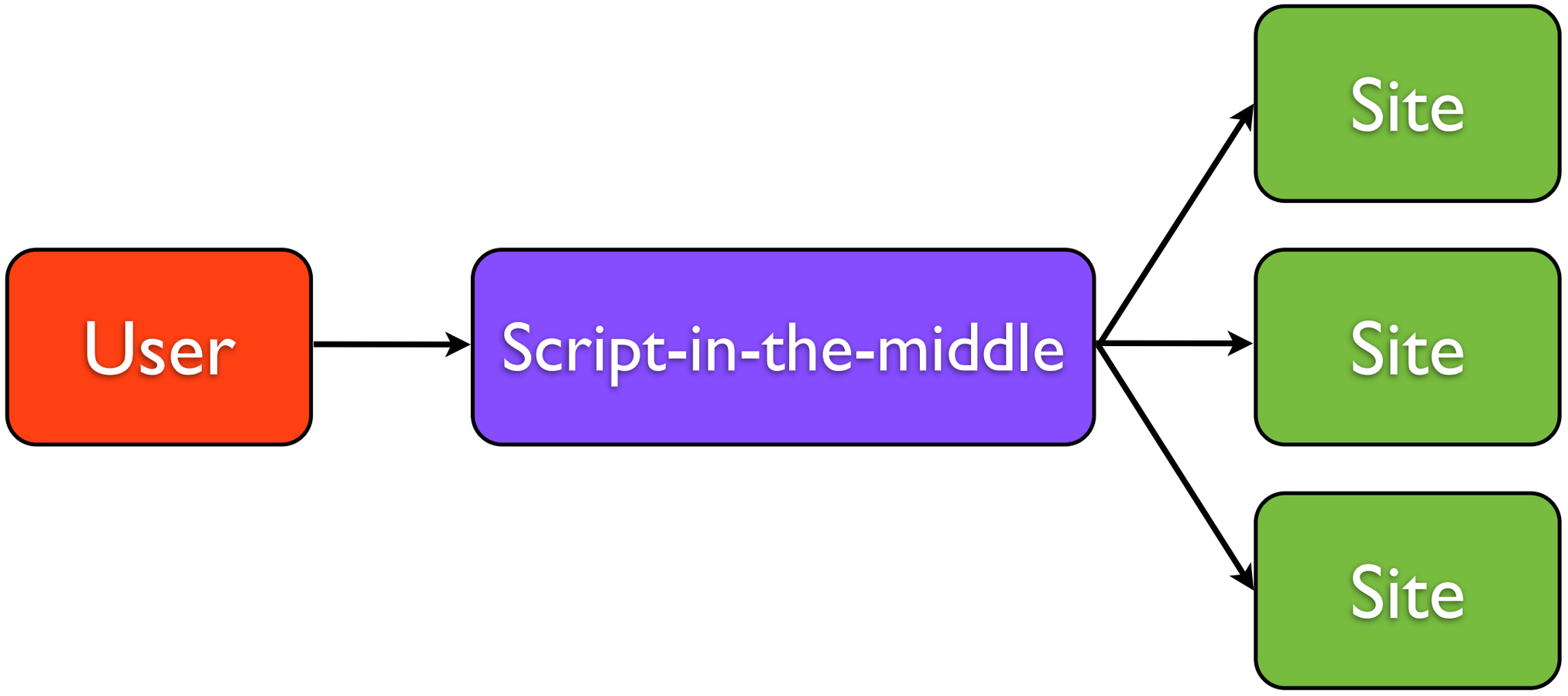
TREND MICRO™

max_goncharov@trendmicro.com
@ppats77

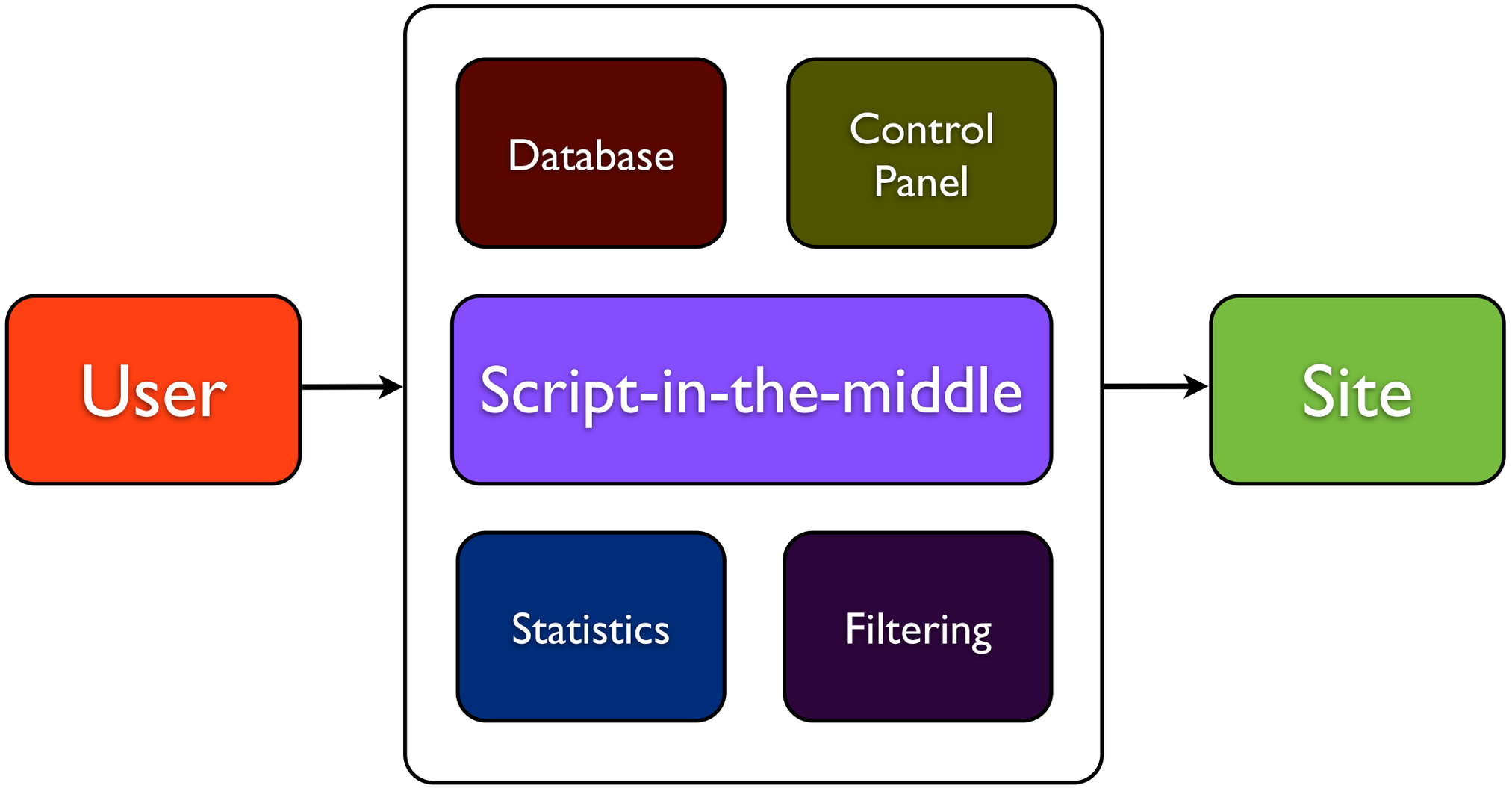
What is web traffic?



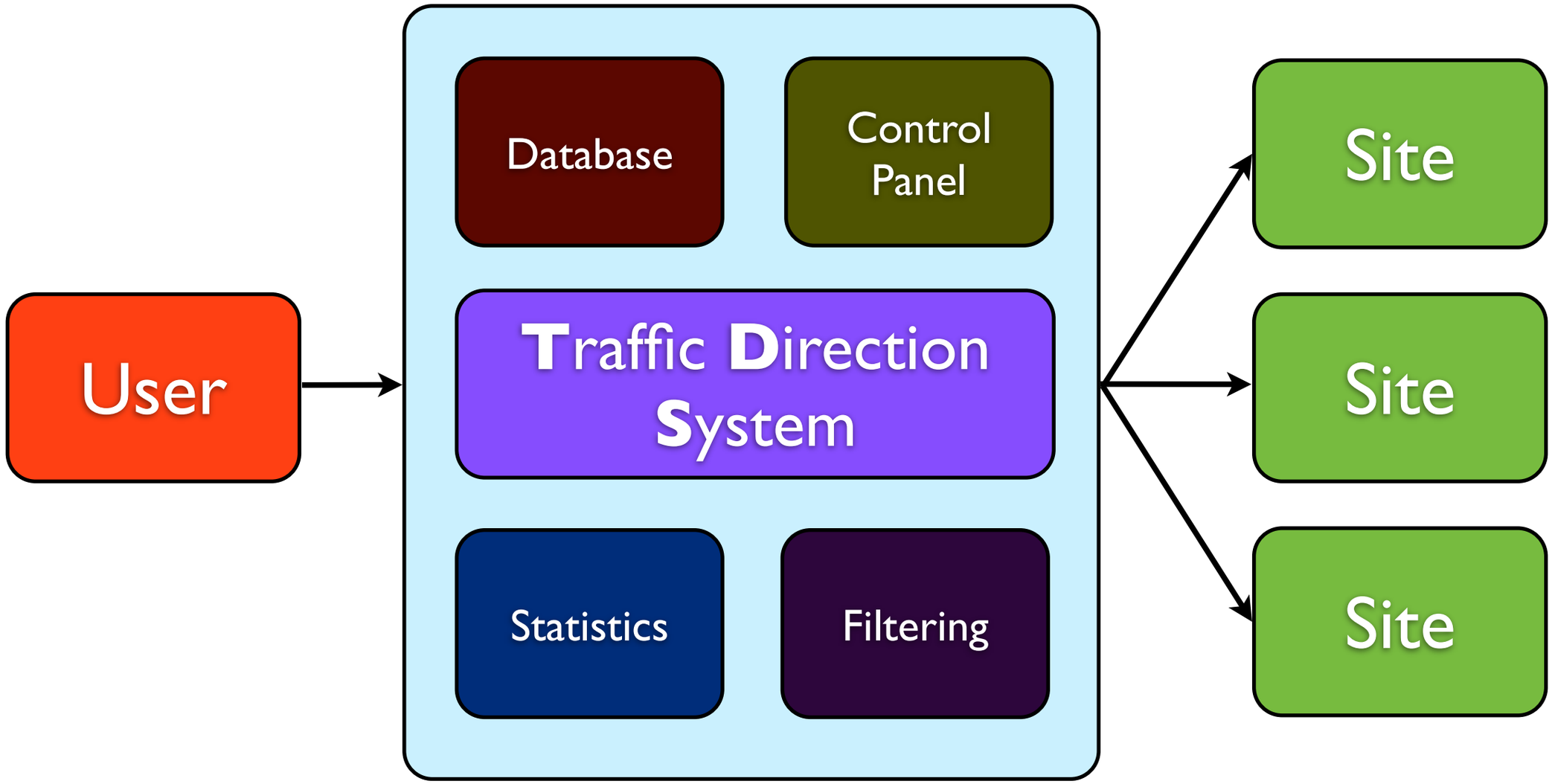
Separate Web traffic ?



System to separate traffic?



Traffic Direction System?



Fingerprint

referer

GET /1/1/typical.php HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, application/x-shockwave-flash, */*
Referer: http://www.trendmicro.com/news
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727)
Host: www.just-a-stie.com
Connection: Keep-Alive

language

browser

OS

Main TDS functionality

Traffic **D**irection **S**ystem

Main TDS functionality

Traffic **D**irection **S**ystem

Control traffic directions

By Browser

By OS

By Geo location

By Time

By Referrer

Main TDS functionality

Traffic **D**irection **S**ystem

Control traffic directions

- By Browser
- By OS
- By Geo location
- By Time
- By Referrer

Filter non wished traffic

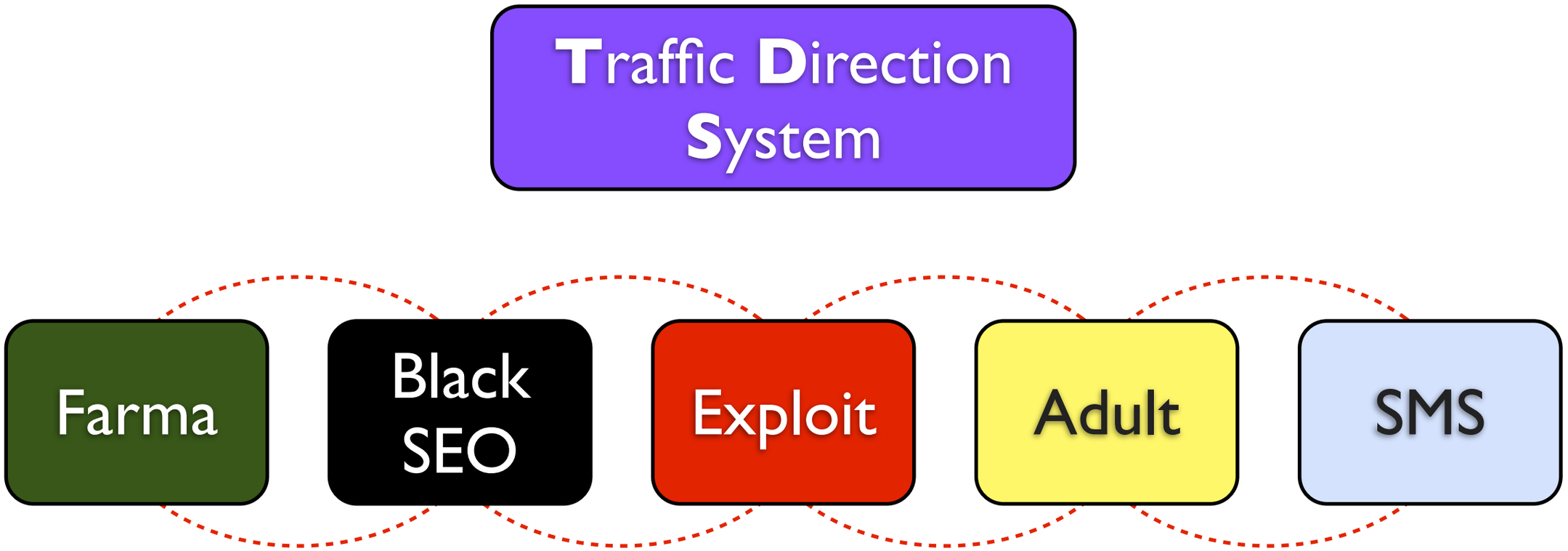
- By Know IP Subnets
- By Search Engine Ref.
- By already seen IPs

Main TDS functionality

Traffic **D**irection **S**ystem

- Control traffic directions
  - By Browser
  - By OS
  - By Geo location
  - By Time
  - By Referrer
- Filter non wished traffic
  - By Know IP Subnets
  - By Search Engine Ref.
  - By already seen IPs
- Collect statistics
  - For Partnerka
  - For Referrals
  - Into Database

Areas of usage.



Volume makes money

Traffic **D**irection **S**ystem

Web User Fraud : <IFrame/>

iframe

max_goncharov@trendmicro.com
@ppats77

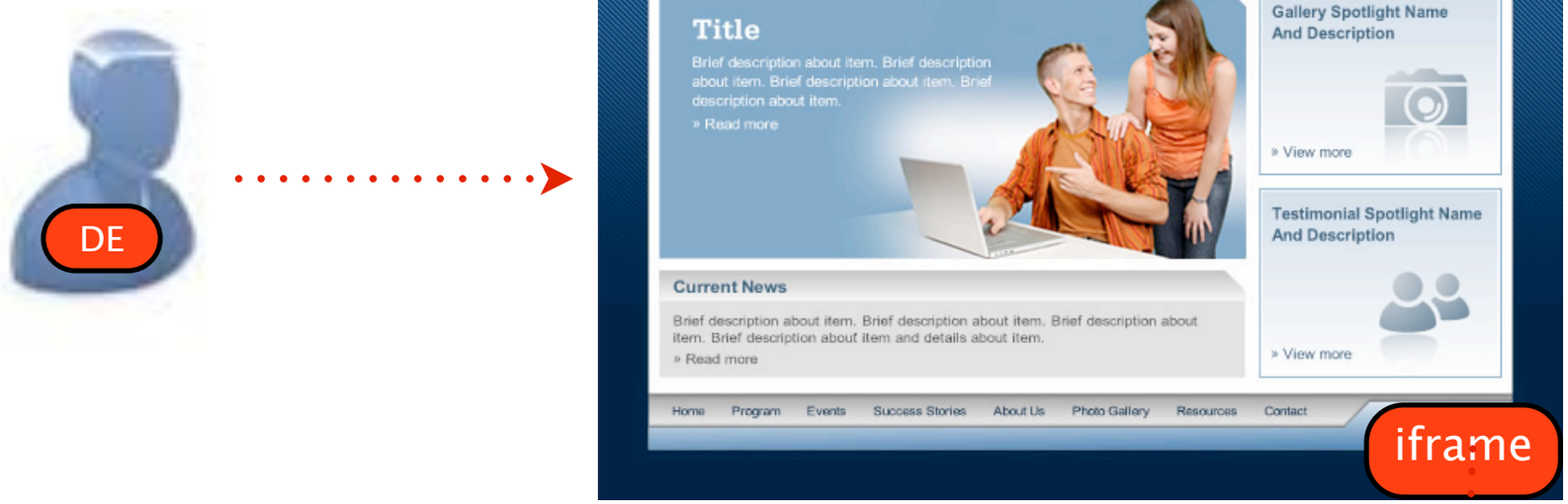
Web User Fraud : <IFrame/>

max_goncharov@trendmicro.com
@ppats77

TDS Traffic Direction System

VB2011 - the 21st Virus Bulletin International

Web User Fraud : <IFrame/>

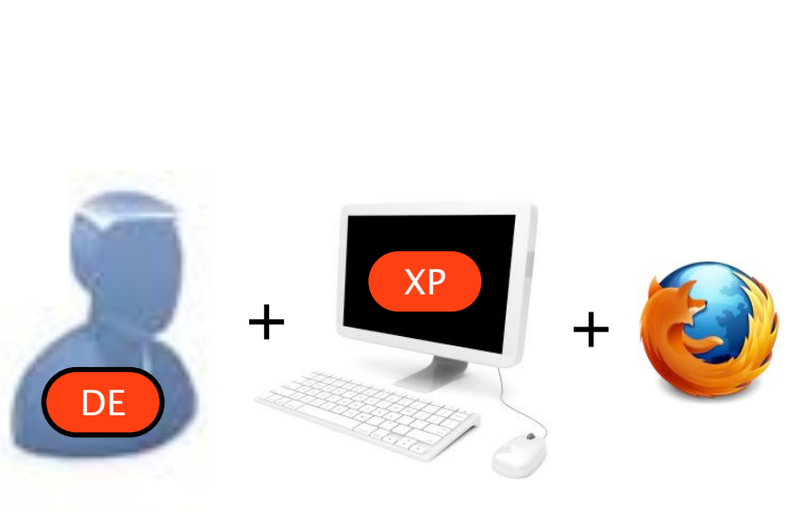


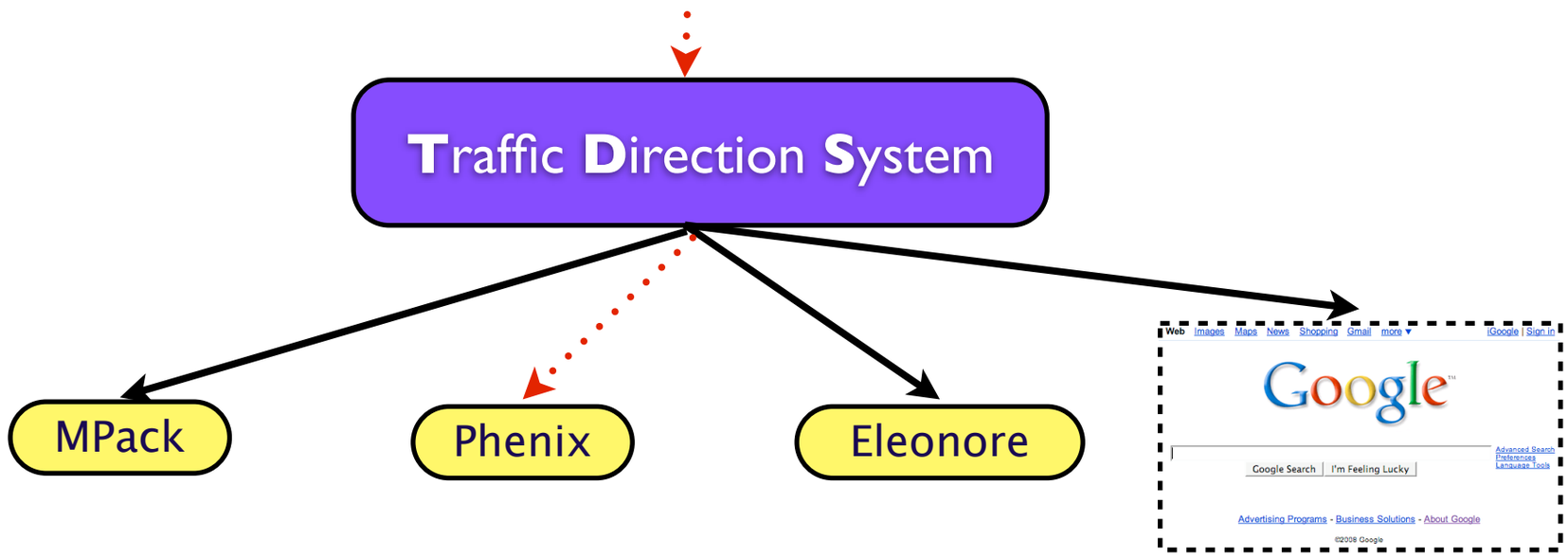
max_goncharov@trendmicro.com
@ppats77

Web User Fraud : <IFrame/>

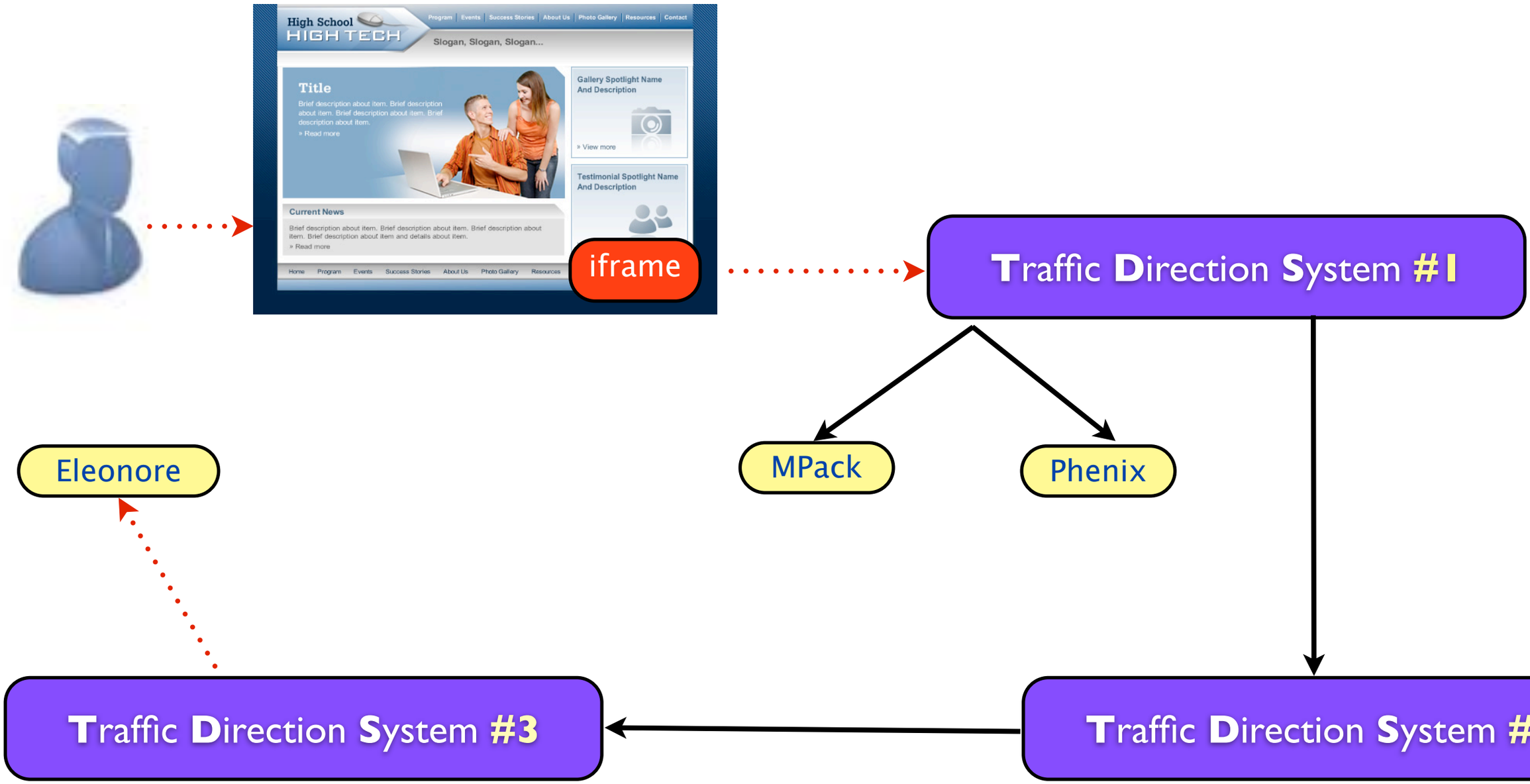
Web User Fraud : <IFrame/>

Malware Vector TDS





Malware Vector multi layer TDS



Partnerka - Possible fraud

Partnerka is an affiliate marketing program, in which the partners are payed off for online distribution of legal or illegal content.

TDS Partnerka - Possible fraud

TDS Partnerka is an affiliate marketing program, in which the partners are payed off for exchange of the **Web Traffic and its monetization**

TDS Partnerka - Possible fraud

AD | LABS MEDIA NETWORK

Live-advert

MegaFotka.net

BITCASH
КОНВЕРТ ФАЙЛОВОГО ТРАФИКА

BODY CLICK

ProTraf v2

Trafoff.org
Bodyclick трафик

StimulProfit.com
Лучший конверт download трафика

Gold-wm.ru

igtraff.com

VIP-TRAFFIC.RU
Пусть сайт работает на тебя

DailyCash
DailyCash.Ru

TRAFFCASH.NET

SunBucks

REALTRAF.RU

TeaserNet.

Wizard TRAFFIC
Мы выкупаем ClickUnder, PopUnder, ICQ Windows

THE GREEN PPC
The Green Pay per Click

TDS Software

Web Server

Application

Database

TDS Software

Simple TDS
Sutra TDS
Crazy TDS
Kalisto TDS
ILTDS
Advanced TDS
Keitaro TDS

max_goncharov@trendmicro.com
@ppats77

TDS Software

- Simple TDS
- Sutra TDS
- Crazy TDS
  Kalisto TDS
- ILTDS
  Advanced TDS
- Keitaro TDS

White to Black

AD | LABS MEDIA NETWORK

Sutra TDS

igtraff.com

Sutra TDS

BITCASH
КОНВЕРТ ФАЙЛОВОГО ТРАФИКА

Sutra TDS

TRAFFCASH.NET

Simple TDS

VIP-TRAFFIC.RU
Пусть сайт работает на тебя

Simple TDS

Traffic Fraud using TDS

intentional

traffic sold to PPI

unintentional

traffic sold to the traffic market

traffic paid as usage fee of the TDS software

traffic paid as usage fee of the TDS service

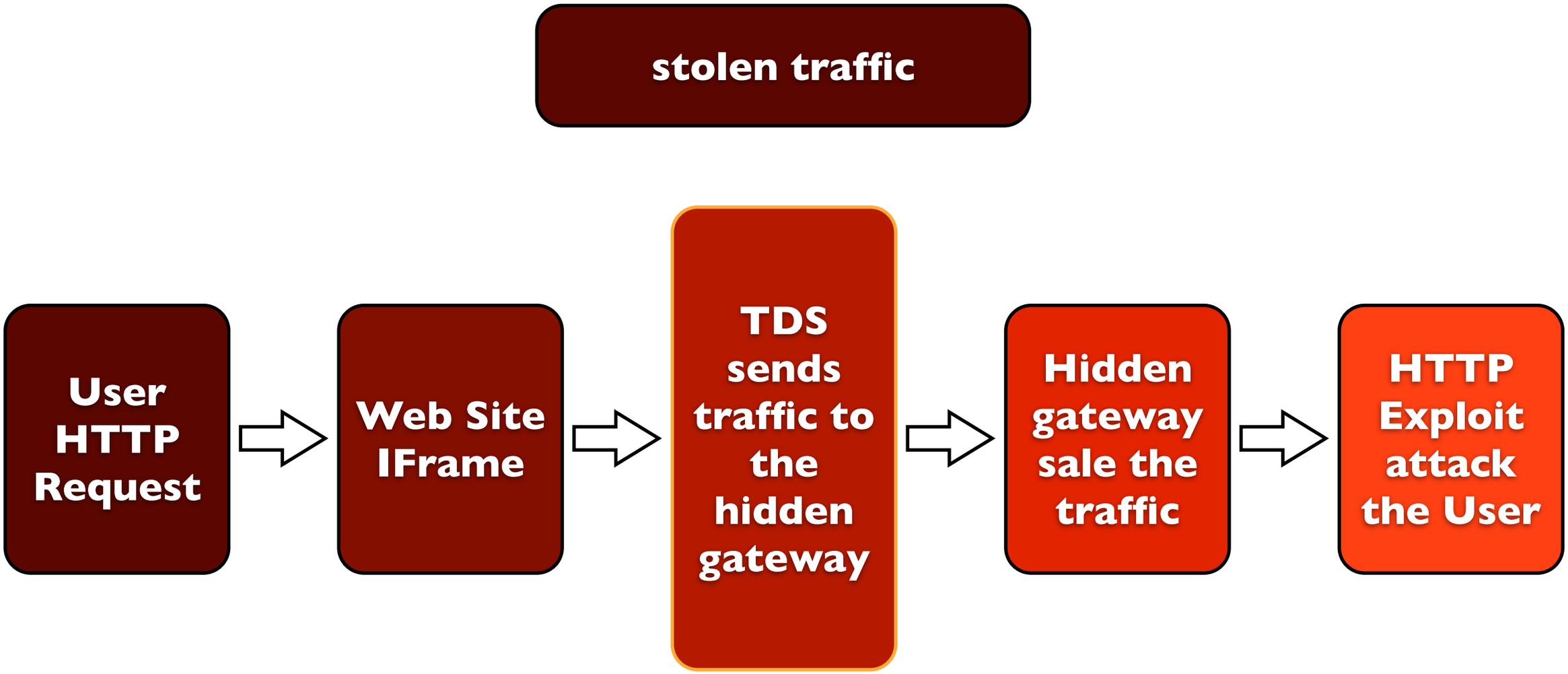
stolen traffic

Traffic Fraud using TDS

traffic sold to the traffic market

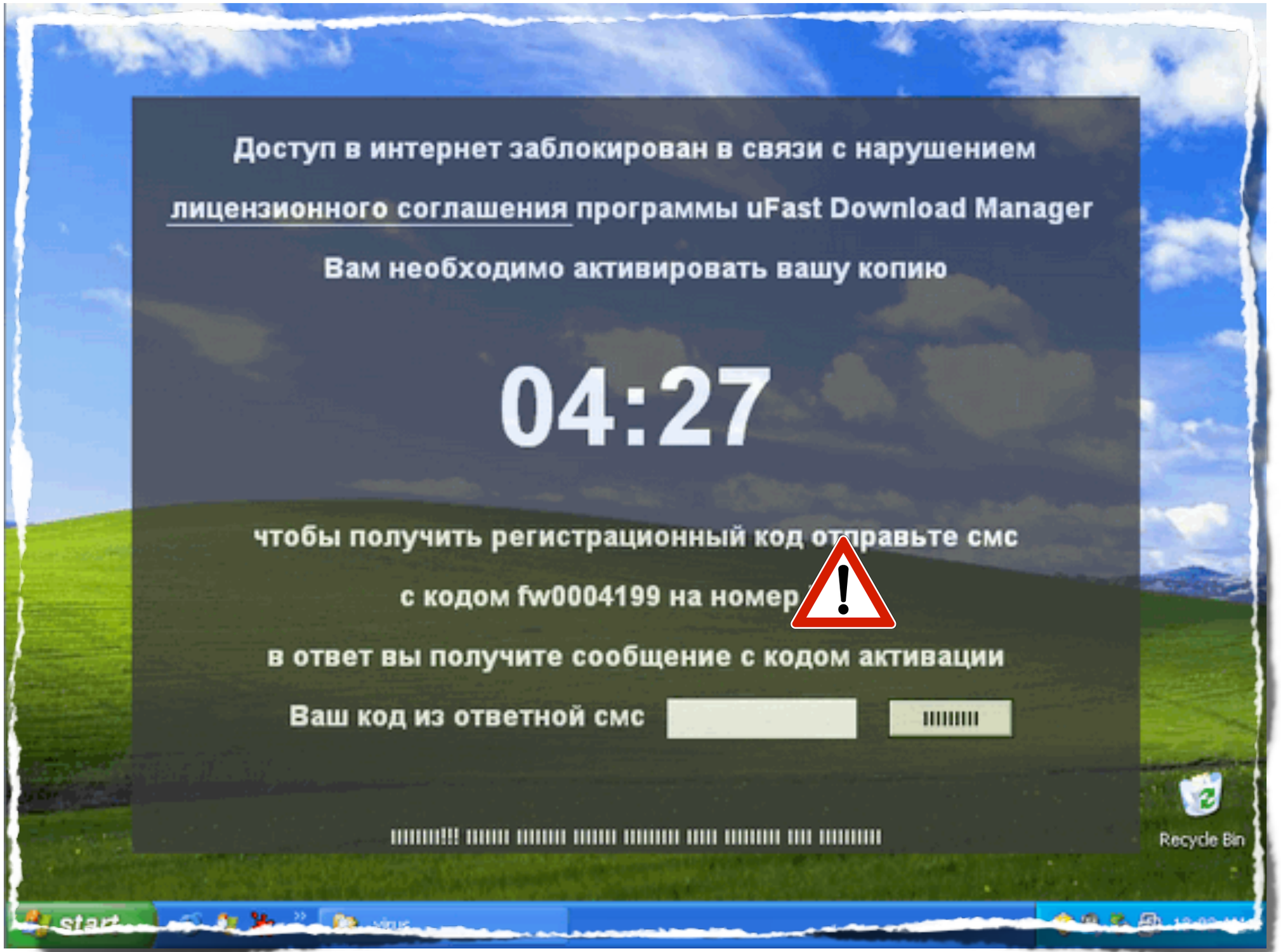
max_goncharov@trendmicro.com
@ppats77

Traffic Fraud using TDS

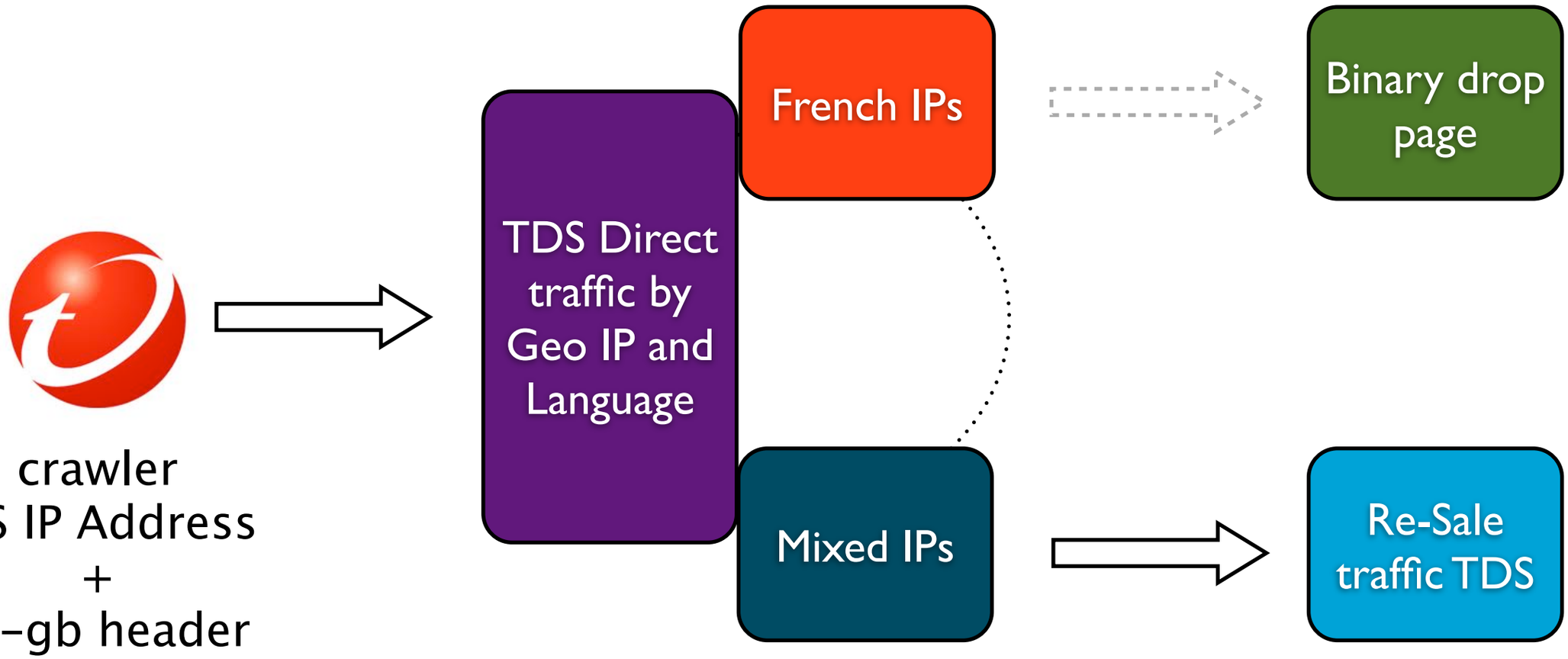


max_goncharov@trendmicro.com
@ppats77

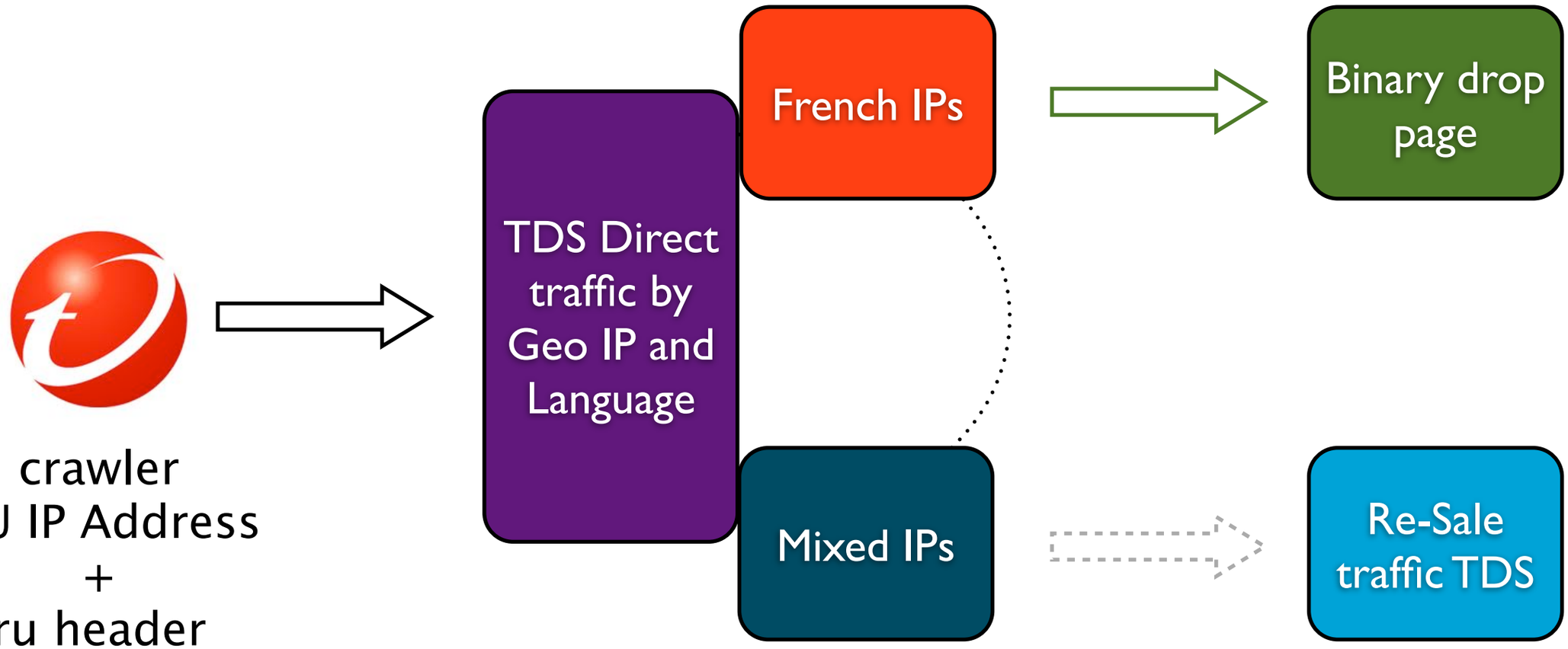
TDS for ransomware



Ransomware example



Ransomware example



Detecting TDS

request

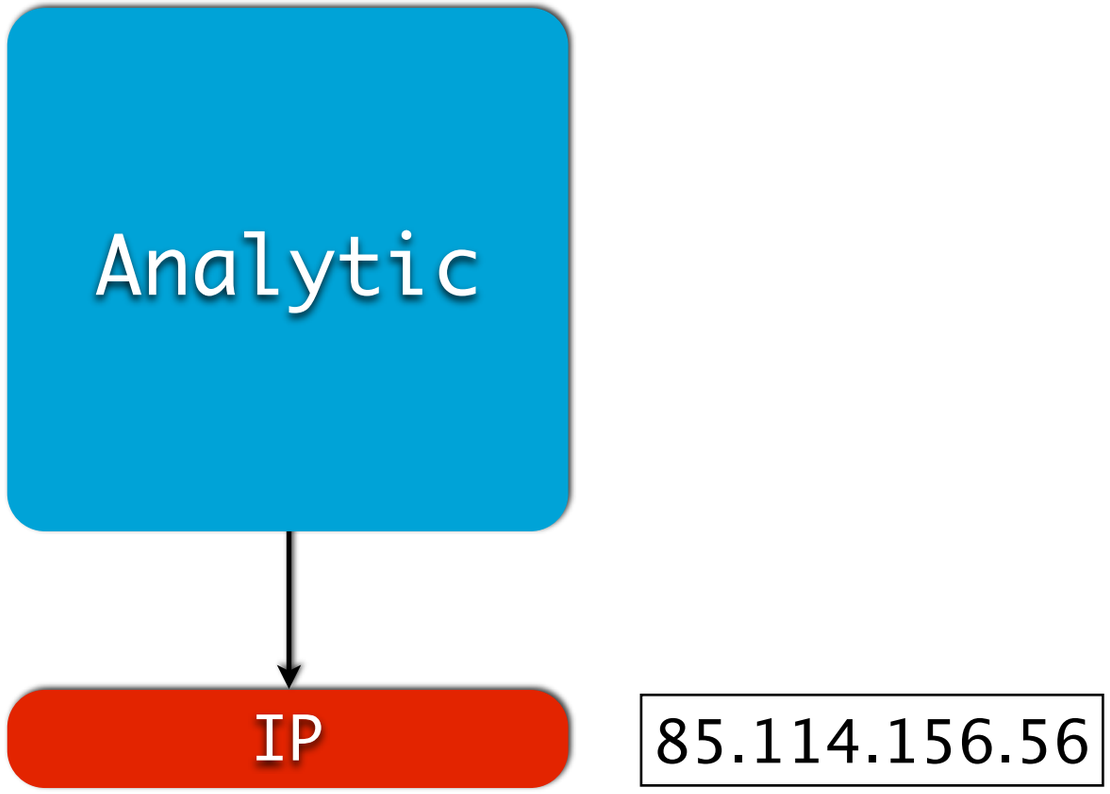
Analytic

Synthetic

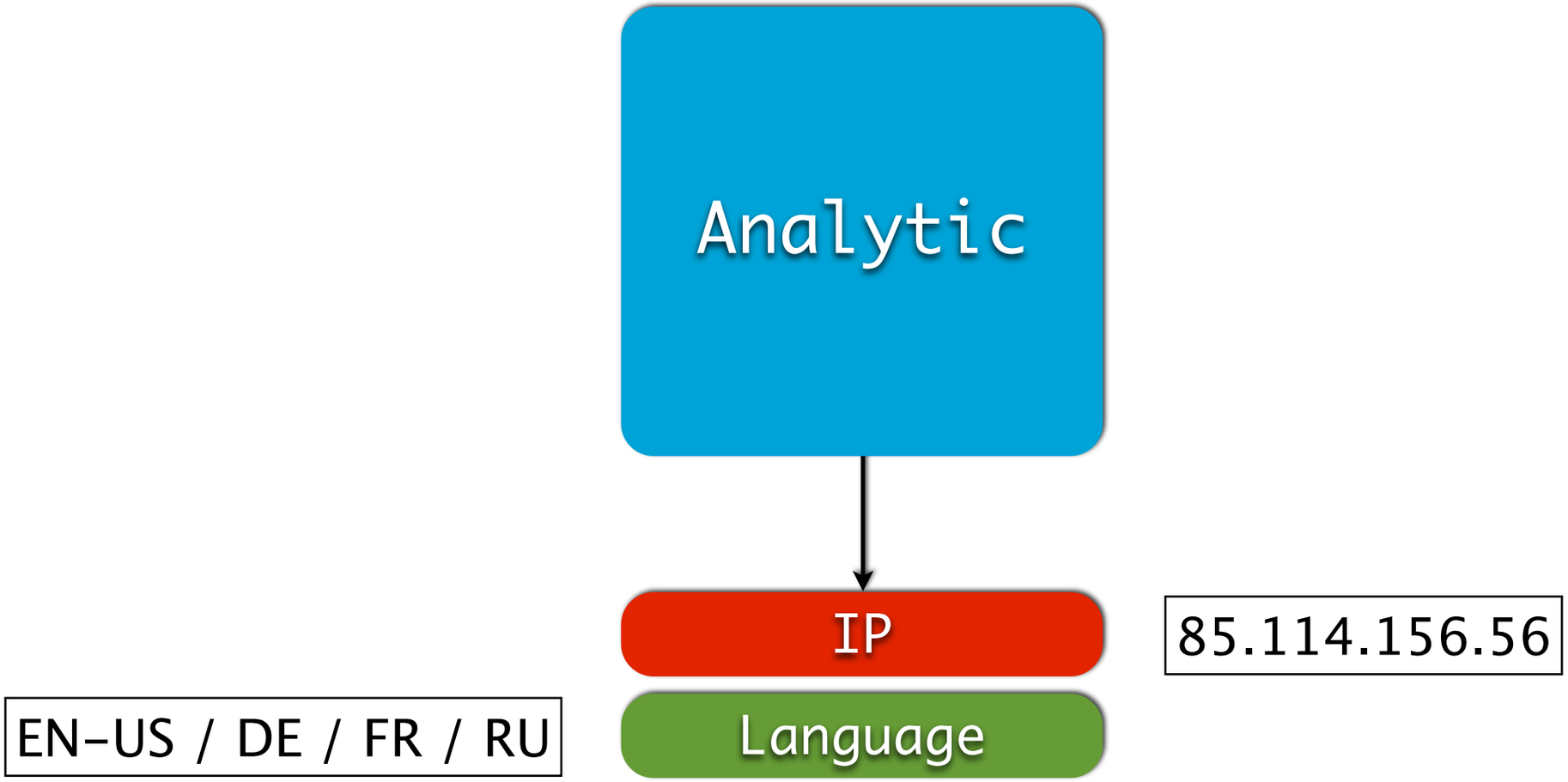
result

Detecting TDS

Detecting TDS

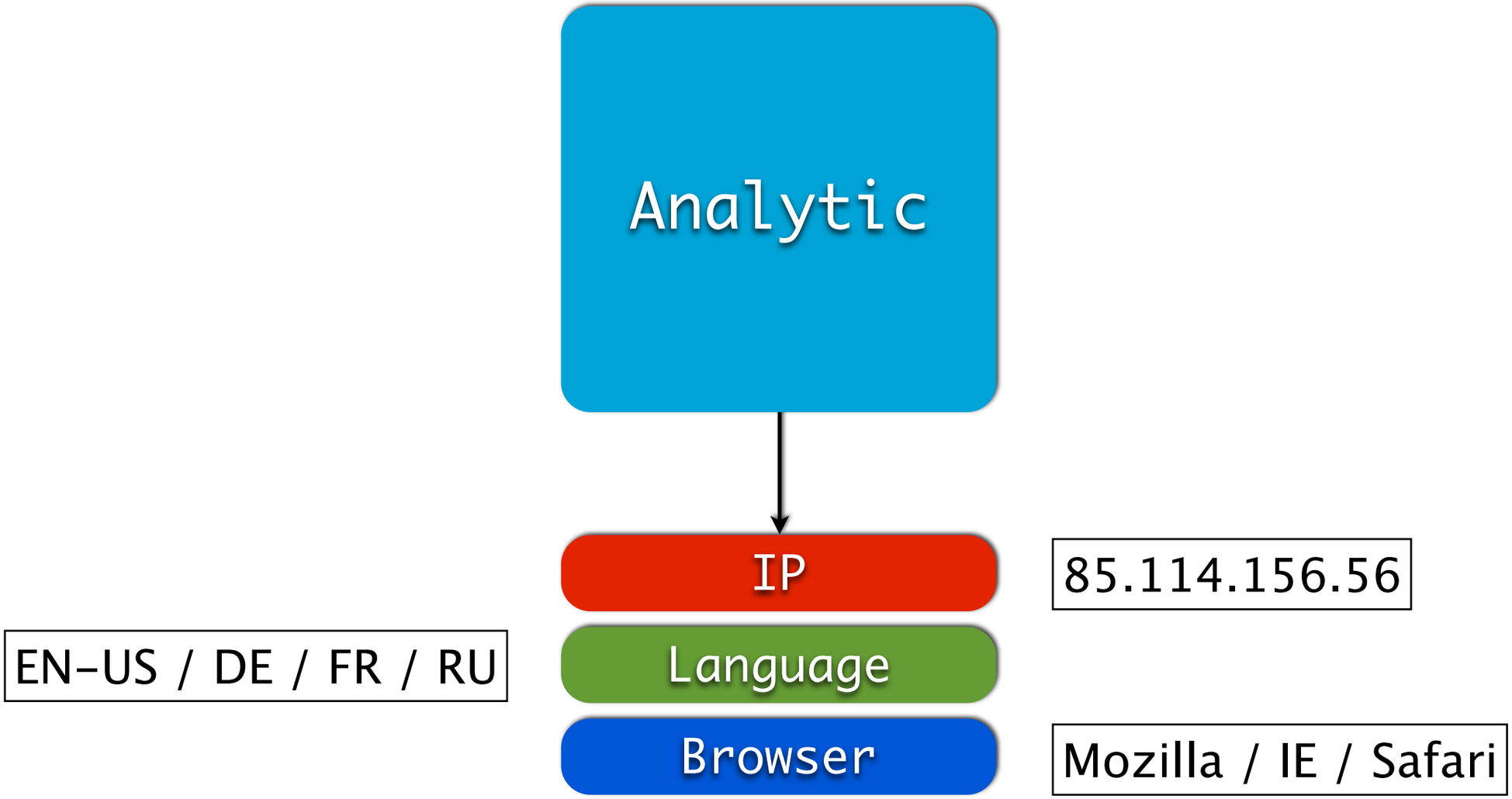


Detecting TDS



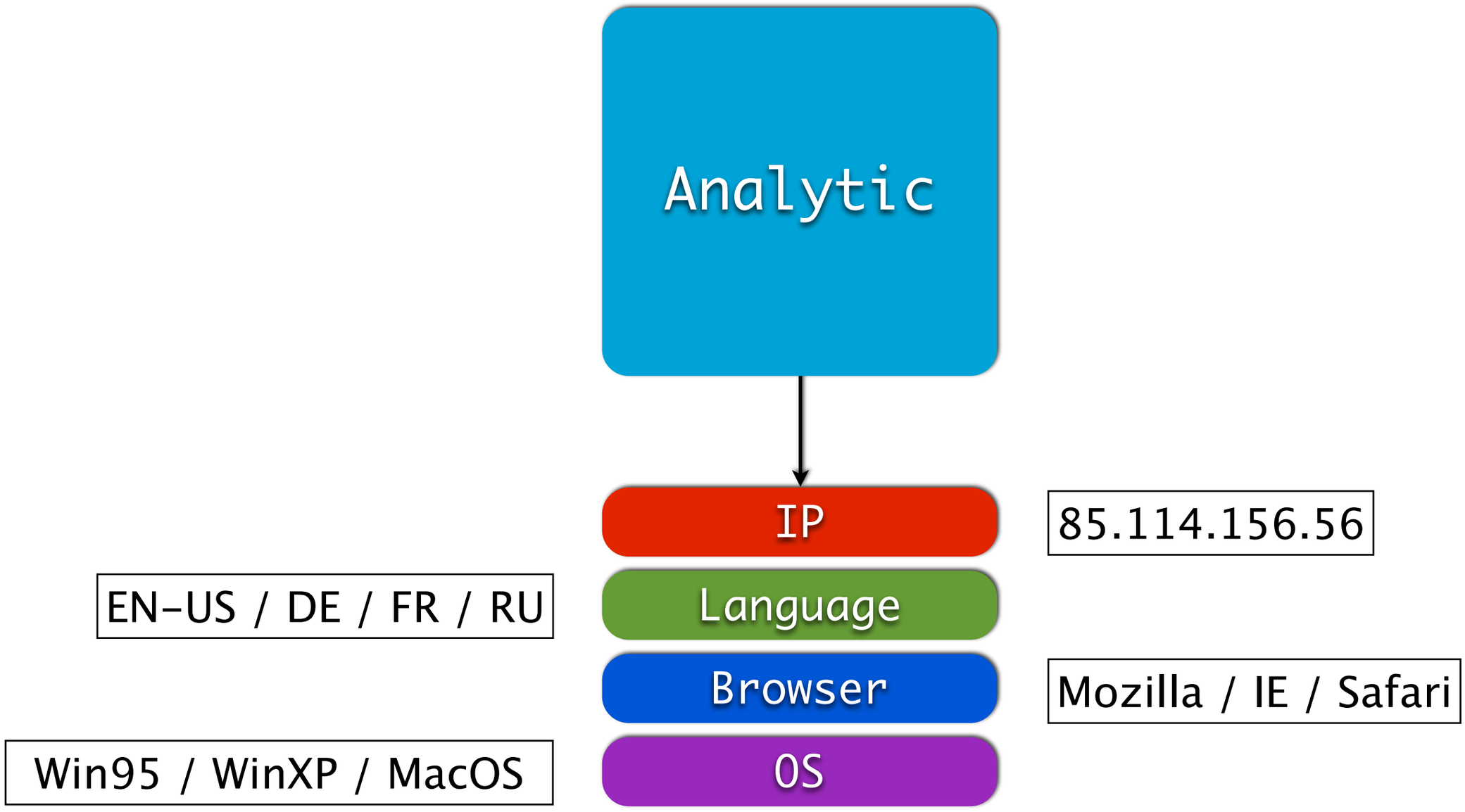
max_goncharov@trendmicro.com
@ppats77

Detecting TDS



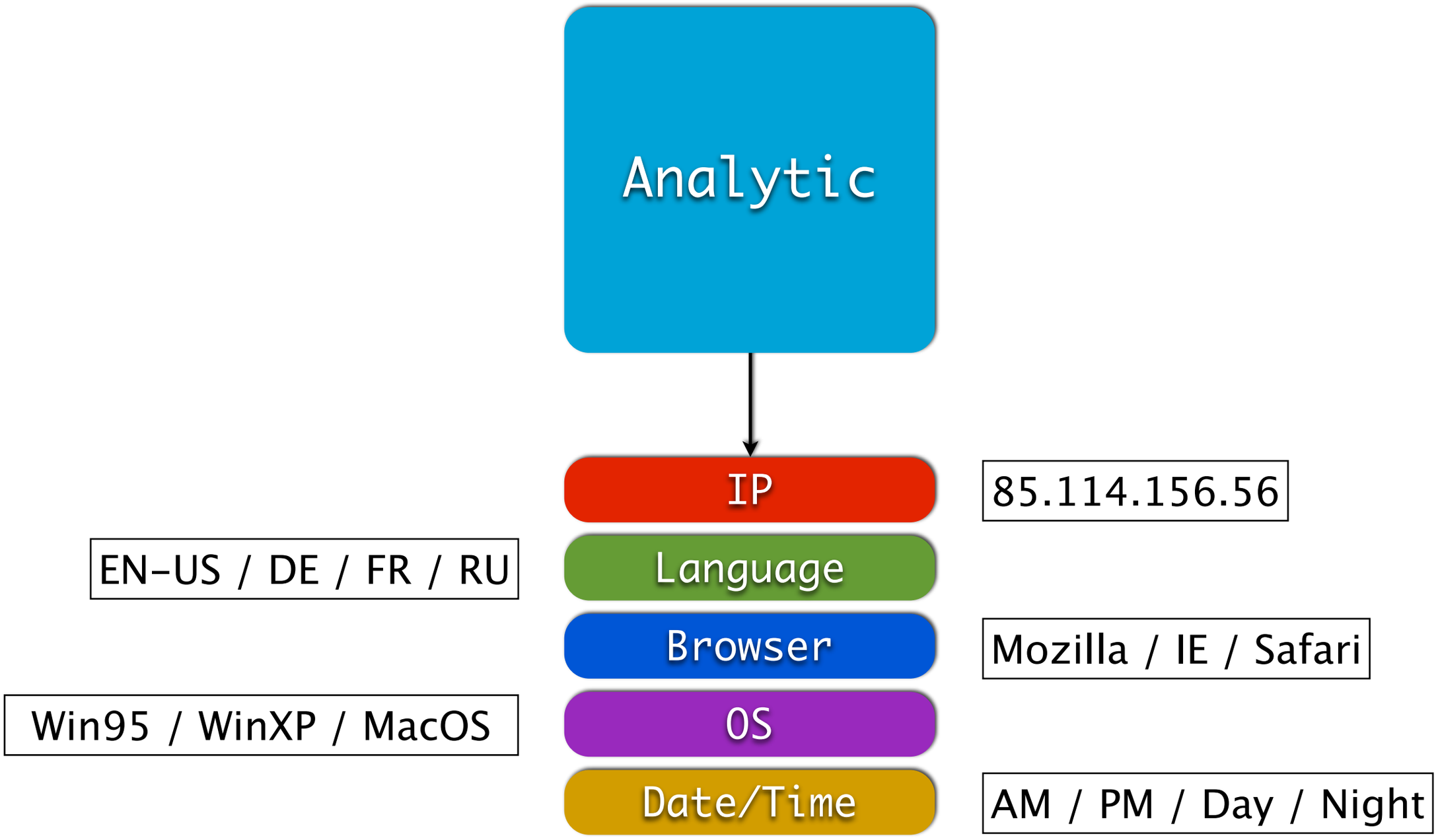
max_goncharov@trendmicro.com
@ppats77

Detecting TDS



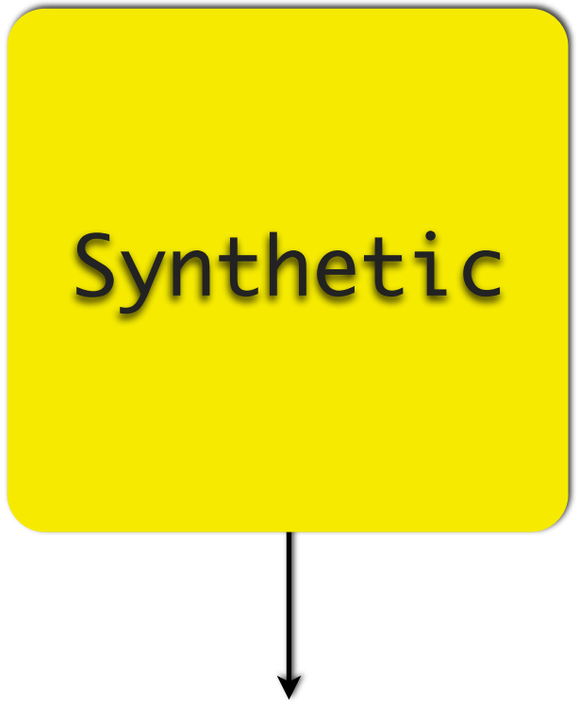
max_goncharov@trendmicro.com
@ppats77

Detecting TDS



max_goncharov@trendmicro.com
@ppats77

Detecting TDS



Detecting TDS

Synthetic

http://domain.com/path

Web Server Structure

Detecting TDS

Synthetic

http://domain.com/path

Web Server Structure

Known File Names

README.txt Version.TXT

Detecting TDS

Synthetic

http://domain.com/path

Web Server Structure

Known File Names

README.txt Version.TXT

/config/ /logs/ /temp

Known Folder Names

Detecting TDS

Synthetic

Web Server Structure

http://domain.com/path

Known File Names

README.txt Version.TXT

Known Folder Names

/config/ /logs/ /temp

Variable Names

GET /go.php?q=1

Statistics: Top 25 Hosts

Host	Number of counts
ranks1.apserver.net	810803
tr-af.com	14293
cloudaway.com	14260
0930sb.ranks1.apserver.net	11057
lxtraffic.com	8358
webmail.bluewin.ch	7726
p8238.adskape.ru	6942
houmekredit.ru	5858
h46r.com	5477
www.picter.jp	5121
www.highqualitysearch.com	4763
p103705.adskape.ru	4260
www.japanesegirlfucked.com	3967
home-sd.com	3876
www.servedadbutler.com	3812
log3.ziyu.net	3806
webmail.sso.bluewin.ch	3765
sexy-tube-site.com	3733
97.64.112.140	3702
uniangel.info	3687
www.sublimedirectory.com	3662
www.youngerbabes.com	3509
www.asian1tube.com	3328
sexonane.ranks1.apserver.net	3324
log5.ziyu.net	3259

Statistics: Top 25 Countries

Country	Number of hits
Japan	407110
United States	212639
Netherlands	135929
N/A	70764
United Kingdom	24908
Germany	12199
Russian Federation	6526
Czech Republic	2791
Ukraine	2711
Switzerland	2471
Asia/Pacific Region	1787
Cyprus	1525
Panama	1191
Australia	1106
Virgin Islands, British	933
Canada	926
France	917
Belgium	816
Latvia	803
Italy	786
Sweden	774
Europe	687
Romania	661
Hong Kong	361
Denmark	241

Statistics: Top 25 Cities

City	Hits
Osaka	394601
N/A	205146
Amsterdam	48282
Ashburn	42893
Dallas	23455
Fort Lauderdale	15159
Providence	13811
Seattle	13010
Weehawken	9363
Miami	8995
Secaucus	8349
Sakura	7605
Atlanta	6400
Herndon	6281
Saint Louis	6241
London	5505
Scranton	5201
Waltham	4930
Houston	4684
Sayreville	3820
San Diego	3342
Moscow	3028
West Palm Beach	2909
Rotterdam	2818
New York	2763

Statistics: Top 25 ISPs

ISP	Hits
SAKURA Internet Inc.	402394
N/A	267485
Warp Link GmbH	41813
Ocom B.V.	26203
HALDEX	22574
Real International Business Corp.	13886
Adelphia	9566
UUNET Technologies	9521
Marconi Communications North America	6998
Beyond The Network Access	6267
ICG NetAhead	5353
Saturnus Breedband Internet B.V.	4704
US Net Incorporated	4669
Global Net Access, LLC	4495
Reflected Networks	4440
Teligent	3418
WebaZilla, Ltd.	3234
Interserver	2989
Syncordia	2901
Productivity OnLine	2707
Swisscom Fixnet AG	2403
EZZI.NET	2181
SC My Computer SRL	2028
Asia Netcom Corporation	1789
NetTransactions, LLC	1470

Conclusion

Traffic Direction Services

New form of underground business

Really difficult to observe

Mixed with legitimate traffic resale

Challenge AV industry in investigations/sourcing

Combined targeting

Questions?

Thanks!

Maxim Goncharov

TREND MICRO Inc.

Thanks!

Maxim Goncharov

TREND MICRO Inc.

Thanks!

Maxim Goncharov

TREND MICRO Inc.