

# This time

On top of the stack

**Application-layer  
security**

Peering into

**Underground  
Economies**

On top of the stack  
**Application-layer**  
**security**

# Application layer

- Familiar faces:
  - HTTP (web)
  - SMTP (mail)
  - Skype
  - Bittorrent
  - Gaming .....
- All of these choose explicitly from the layer beneath them (UDP vs TCP)
  - TCP when you must have reliable, in-order delivery
    - Web, mail, BitTorrent
  - UDP when you prefer timeliness over reliability
    - Gaming, Skype

# In what layer should security go?

- Fundamental principle: the **end-to-end principle**  
(applies to reliability in general)
- If there is a function that can be implemented correctly and completely only at the end hosts, then put it there, not in the network.
  - Exception: the network can be used as a performance enhancement
- How can TCP know what it means to secure your application?
  - Does it just need encryption? Key sharing? Obfuscated timing? ....?

# Example: SMTP (RFC 821)

---

## Example of the SMTP Procedure

This SMTP example shows mail sent by Smith at host Alpha.ARPA, to Jones, Green, and Brown at host Beta.ARPA. Here we assume that host Alpha contacts host Beta directly.

```
S: MAIL FROM:<Smith@Alpha.ARPA>  
R: 250 OK
```

```
S: RCPT TO:<Jones@Beta.ARPA>  
R: 250 OK
```

```
S: RCPT TO:<Green@Beta.ARPA>  
R: 550 No such user here
```

```
S: RCPT TO:<Brown@Beta.ARPA>  
R: 250 OK
```

```
S: DATA  
R: 354 Start mail input; end with <CRLF>.<CRLF>  
S: Blah blah blah...  
S: ...etc. etc. etc.  
S: <CRLF>.<CRLF>  
R: 250 OK
```

The mail has now been accepted for Jones and Brown. Green did not have a mailbox at host Beta.

Example 1

---

# Example: SMTP (RFC 821)

---

## Example of the SMTP Procedure

This SMTP example shows mail sent by Smith at host Alpha.ARPA, to Jones, Green, and Brown at host Beta.ARPA. Here we assume that host Alpha contacts host Beta directly.

```
S: MAIL FROM:<Smith@Alpha.ARPA>
R: 250 OK

S: RCPT TO:<Jones@Beta.ARPA>
R: 250 OK

S: RCPT TO:<Green@Beta.ARPA>
R: 550 No such user here

S: RCPT TO:<Brown@Beta.ARPA>
R: 250 OK

S: DATA
R: 354 Start mail input; end with <CRLF>.<CRLF>
S: Blah blah blah...
S: ...etc. etc. etc.
S: <CRLF>.<CRLF>
R: 250 OK
```

The mail has now been accepted for Jones and Brown. Green did not have a mailbox at host Beta.

Example 1

---



These are all just packets  
and you can construct  
whatever packets you want

# In what layer should security go?

- Need to understand what properties you get from each layer
- If you require a property that cannot be guaranteed by the underlying layers, then you have to add it to the “end”
- Email: how would you fix this?
  - You want authentic communication
  - Can you build it out of an unauthenticated channel?

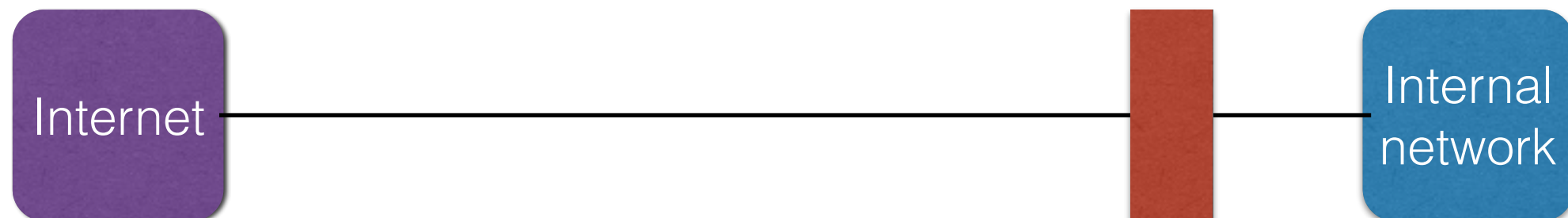
# Protecting your network

- How do you harden a set of systems against an external attack?
- Challenge: attack surface
  - The more network services your machines run, the greater the risk
- One approach: turn off unnecessary network services
  - **But** you have to know all the services
  - And sometimes trusted remote users still require access
- Challenge: scaling to 100s or 1000s of systems



# Scalable solution to management complexity

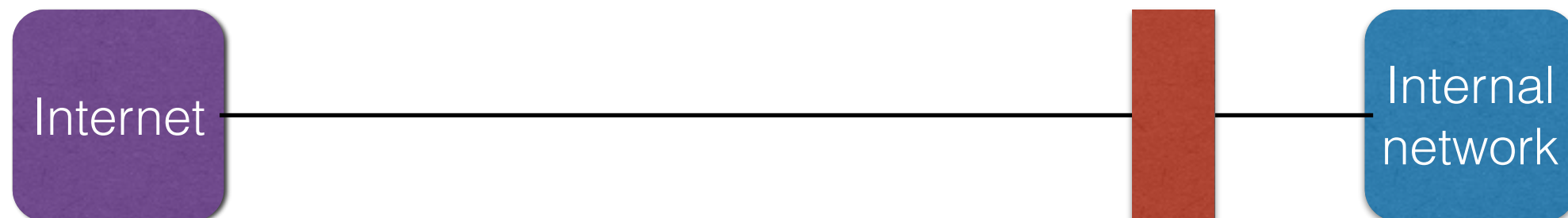
- Reduce risk by blocking from *within the network* any outsiders from having unwanted access
- Interpose a **firewall** as a reference monitor on traffic



# Scalable solution to management complexity

- Reduce risk by blocking from *within the network* any outsiders from having unwanted access
- Interpose a **firewall** as a reference monitor on traffic

What do we know about reference monitors?







# Scalable solution to management complexity

- Reduce risk by blocking from *within the network* any outsiders from having unwanted access
- Interpose a firewall as a reference monitor on traffic

What do we know about reference monitors?

**You must ensure complete mediation**

- Firewalls can typically cover thousands of hosts
  - Need to find a chokepoint in your network
  - Where do chokepoints normally exist?



# Security policies

- Network security policy:
  - what hosts are allowed to talk to what other hosts,
  - and who is allowed to access what service?
- Distinguish between **inbound** and **outbound** connections
  - **Outbound**: internal users accessing external services
  - **Inbound**: external users attempting to connect to services on internal machines
- Why distinguish inbound/outbound?
  - Because it fits with a common **threat model**

# Security policies

- Firewalls permit a conceptually simple **access control policy**
  - Permit *inside* users to connect to any service
  - Restrict *external* users:
- External users:
  - Permit connections to services that are meant to be externally visible
  - Deny connections services that are not meant to be externally visible

# Expressing firewall policies

- Typically represented by a prioritized list of match/action pairs.
  - Perform the action corresponding to the highest-priority rule that matches
- Example actions
  - Allow the traffic to flow
  - Drop the traffic
  - Also possibly rate-limit the traffic
- Matching rules
  - **Traditional firewall**: operates over header data (src-IP, src-port, dst-IP, dst-port, protocol, TCP flags)
  - **Application-layer firewall**: also include application-layer data (perform “*deep packet inspection*” that looks at the payloads, not just the headers)

# Great firewall of China

- Uses many of the same techniques in firewalls
  - What is the difference?
- Also uses “application-layer” firewalls
  - Inspects payloads
    - E.g., requested domain names in DNS queries
  - And can inject application-layer responses to censor
    - E.g., can reply to wikipedia.org DNS query with a lemon IP



# Getting around the Great Firewall of China

# Getting around the Great Firewall of China

- If the src or dst is in the country, then all traffic *must* go through the firewall
  - Common approach: **confidentiality**
    - Countermeasure: block **Tor** traffic (or other encrypted traffic) to all but a specific set of hosts (for businesses who use VPNs)
  - New approach: **protocol obfuscation**
    - Make a protocol the country disallows (e.g., Tor) look like another that the country is ok with (e.g., Skype)
  - New approach: **decoy routing**
    - Make it look like you are talking to destination D but a router on the path redirects you to your true destination D'.

# Getting around the Great Firewall of China

- If the src or dst is in the country, then all traffic *must* go through the firewall
  - Common approach: **confidentiality**
    - Countermeasure: block **Tor** traffic (or other encrypted traffic) to all but a specific set of hosts (for businesses who use VPNs)
  - New approach: **protocol obfuscation**
    - Make a protocol the country disallows (e.g., Tor) look like another that the country is ok with (e.g., Skype)
  - New approach: **decoy routing**
    - Make it look like you are talking to destination D but a router on the path redirects you to your true destination D'.

**Avoiding censorship from a “routing-capable adversary”  
is one of the most challenging open problems**

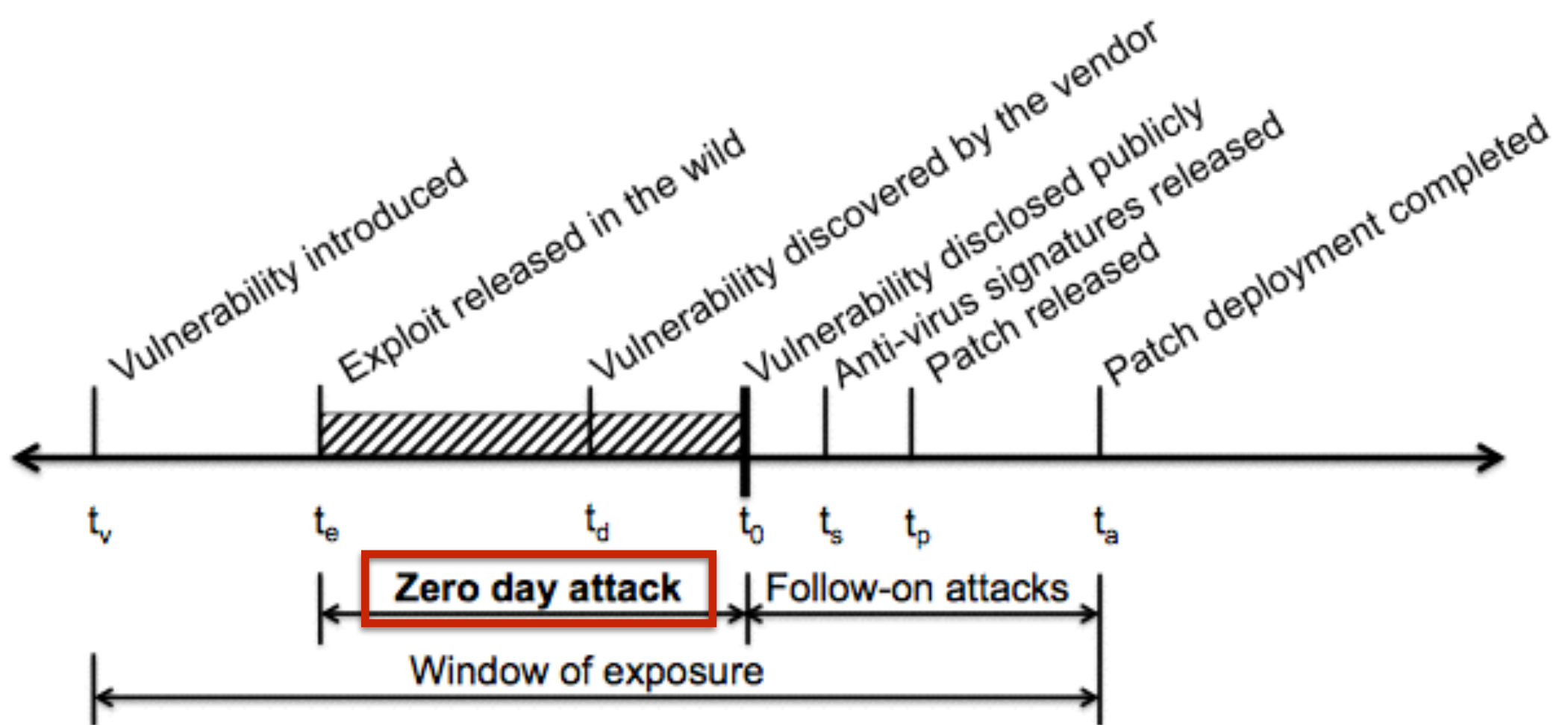
# Getting around the Great Firewall of China

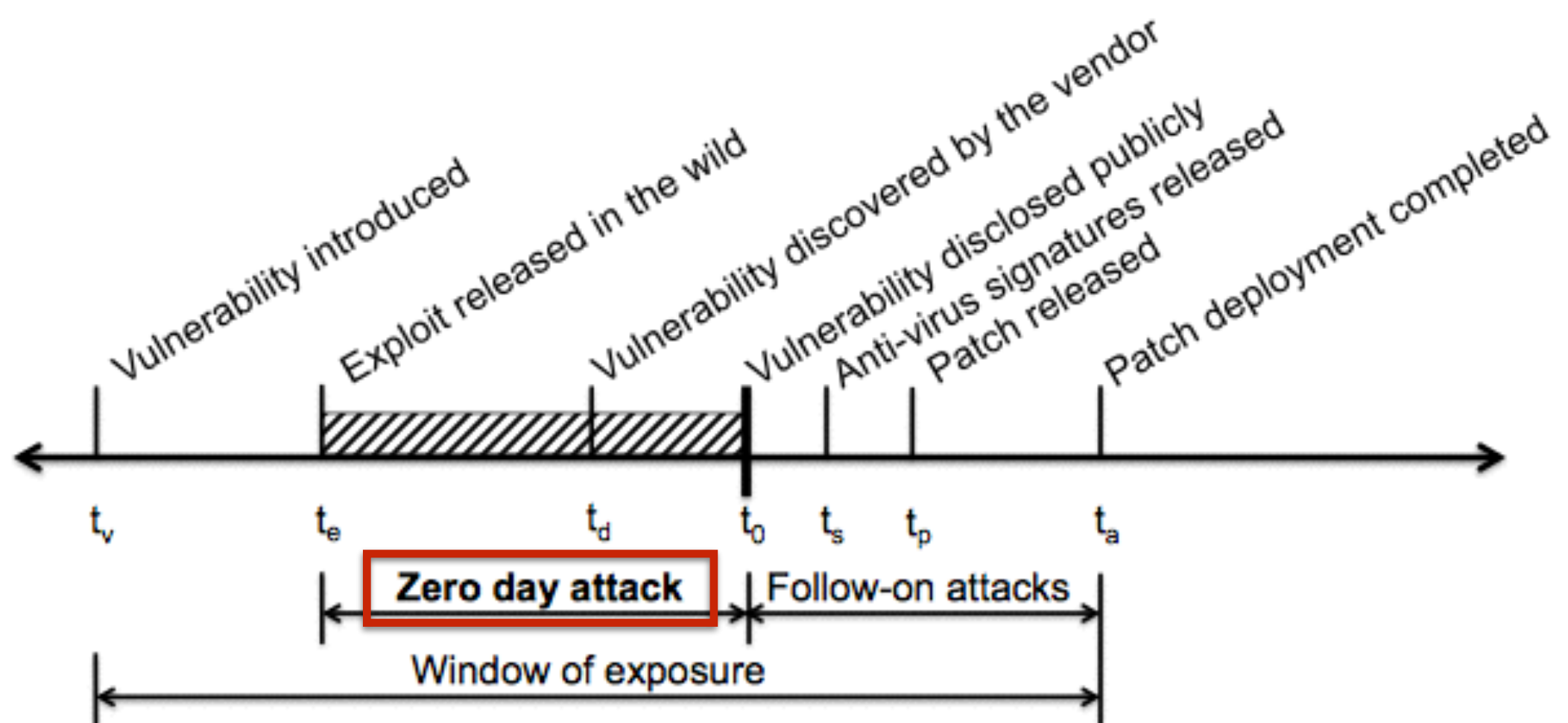
- Even if **neither** source nor destination are in China, they can *still be censored* if their traffic goes *through* China
  - This censorship-in-transit is sometimes called “collateral damage”
  - Similar things elsewhere: “**boomerang routing**” leads, e.g., two hosts in Brazil to have their traffic routed through the US.
  - There is general concern as to what intermediate countries are doing with our traffic
- New approach: “**Alibi routing**”
  - “I want to communicate with destination D but I want proof that my packets avoided these these regions of the world...”

Peering into  
**Underground  
Economies**

# Underground economies

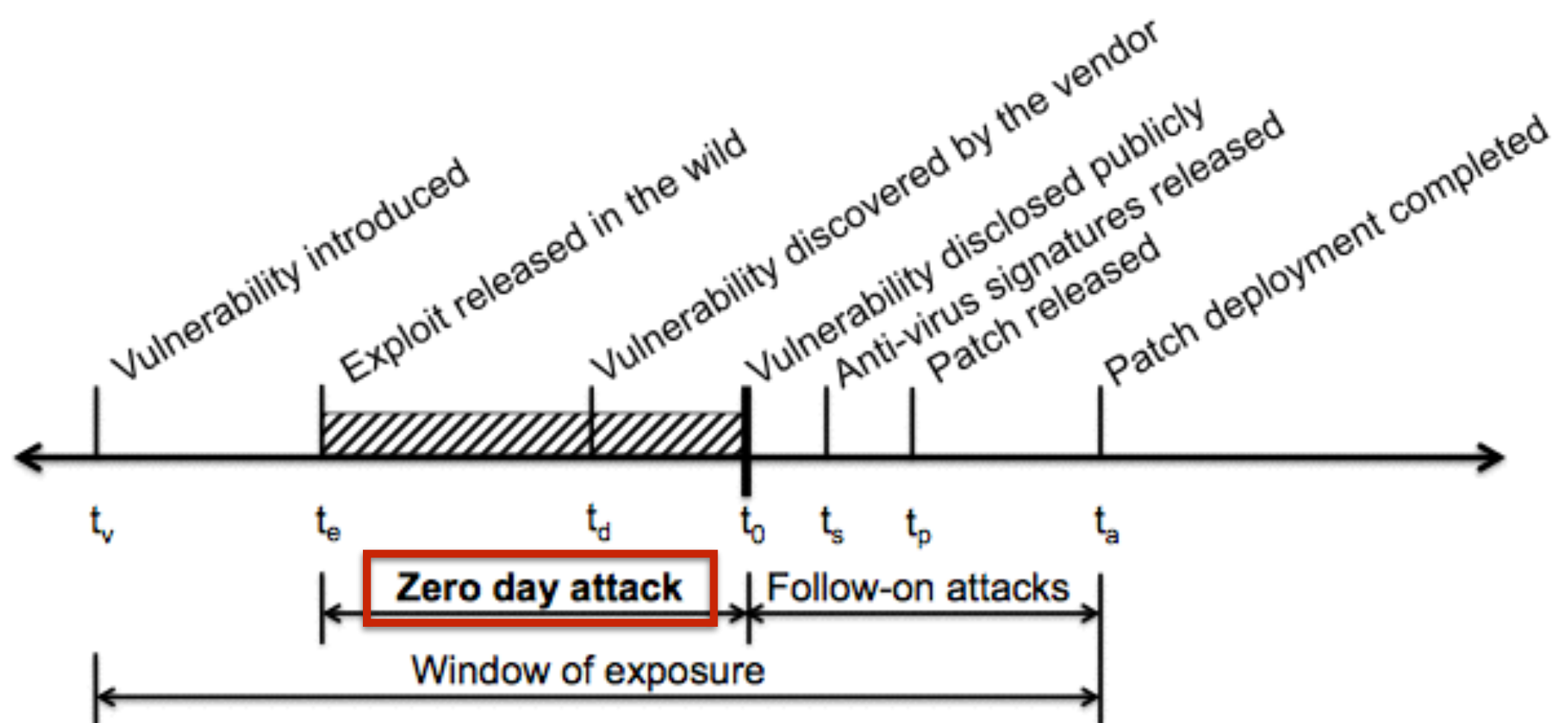
- Economics drives both the attacks and the defenses
- What is for sale? Who sells it? How?
  - Defenders: Antivirus vendors, firewall vendors, etc.
  - *What about the attackers?*
- The idea is that we may be able to stem attacks if we can understand
  - the incentives
  - the choke points (might there be one bank we could shut down to cease spam?)





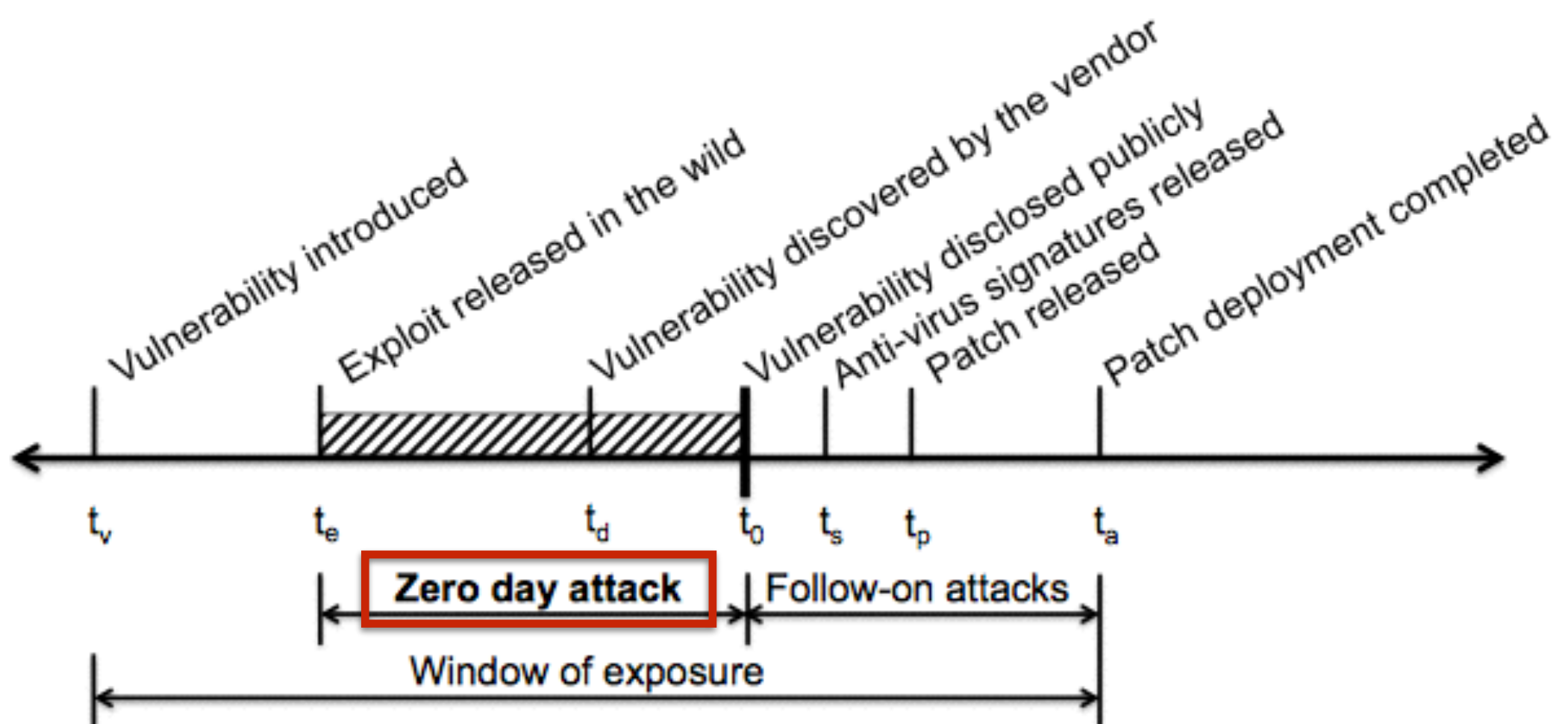
- **Who buys:** Attackers, spies (and the companies who wrote the software) want to know about them
- **Through whom:** anonymous middlemen (e.g. Grusq) who match vulnerability finders up with buyers. Take commission (15% typical).
- **Payment:** Made in installments (cease payment when zero-day over)





- **Who buys:** Attackers, spies (and the companies who wrote the software) want to know about them
- **Through whom:** anonymous middlemen (e.g. Grusq) who match vulnerability finders up with buyers. Take commission (15% typical).
- **Payment:** Made in installments (cease payment when zero-day over)

Google offers a max of \$3133.70 for information about flaws in their tech



- **Who buys:** Attackers, spies (and the companies who wrote the software) want to know about them
- **Through whom:** anonymous middlemen (e.g. Grusq) who match vulnerability finders up with buyers. Take commission (15% typical).
- **Payment:** Made in installments (cease payment when zero-day over)

Google offers a max of \$3133.70 for information about flaws in their tech

ADOBE READER	\$5,000-\$30,000
MAC OSX	\$20,000-\$50,000
ANDROID	\$30,000-\$60,000
FLASH OR JAVA BROWSER PLUG-INS	\$40,000-\$100,000
MICROSOFT WORD	\$50,000-\$100,000
WINDOWS	\$60,000-\$120,000
FIREFOX OR SAFARI	\$60,000-\$150,000
CHROME OR INTERNET EXPLORER	\$80,000-\$200,000
IOS	\$100,000-\$250,000

# Spam

- Unsolicited, annoying email (or posts on blogs, social networks, etc.) that seeks to
  - Sell products
  - Get users to install malicious software
- Typical defenses
  - Look for key words in the messages
  - Block certain senders (SpamHaus blacklist of IP addrs)
- But what is the economics behind it all?
  - How do they send out so much email?
  - Are they selling real things? How?

# Sending spam

- Tons of email to send, and easy to block a single IP address from sending
- Need lots of IP addresses
  - But since SMTP (email) uses TCP, we need to actually be able to operate those IP addresses
- Buy lots of computers? (expensive)

# Sending spam

- Tons of email to send, and easy to block a single IP address from sending
- Need lots of IP addresses
  - But since SMTP (email) uses TCP, we need to actually be able to operate those IP addresses
- Buy lots of computers? (expensive)

**Compromise lots of computers!**

# Botnet

- Collection of compromised machines (bots) under unified control of an attacker (botmaster)
- Method of compromise decoupled from method of control
  - Launch a worm/virus, etc.: remember, payload is orthogonal!
- Upon infection, a new bot “phones home” to *rendezvous* with botnet “command-and-control” (C&C)
- Botmaster uses C&C to push out commands and updates

# Botnet

- Collection of compromised machines (bots) under unified control of an attacker (botmaster)
- Method of compromise decoupled from method of control
  - Launch a worm/virus, etc.: remember, payload is orthogonal!
- Upon infection, a new bot “phones home” to *rendezvous* with botnet “command-and-control” (C&C)
- Botmaster uses C&C to push out commands and updates



# Botnet

- Collection of compromised machines (bots) under unified control of an attacker (botmaster)
- Method of compromise decoupled from method of control
  - Launch a worm/virus, etc.: remember, payload is orthogonal!
- Upon infection, a new bot “phones home” to *rendezvous* with botnet “command-and-control” (C&C)
- Botmaster uses C&C to push out commands and updates

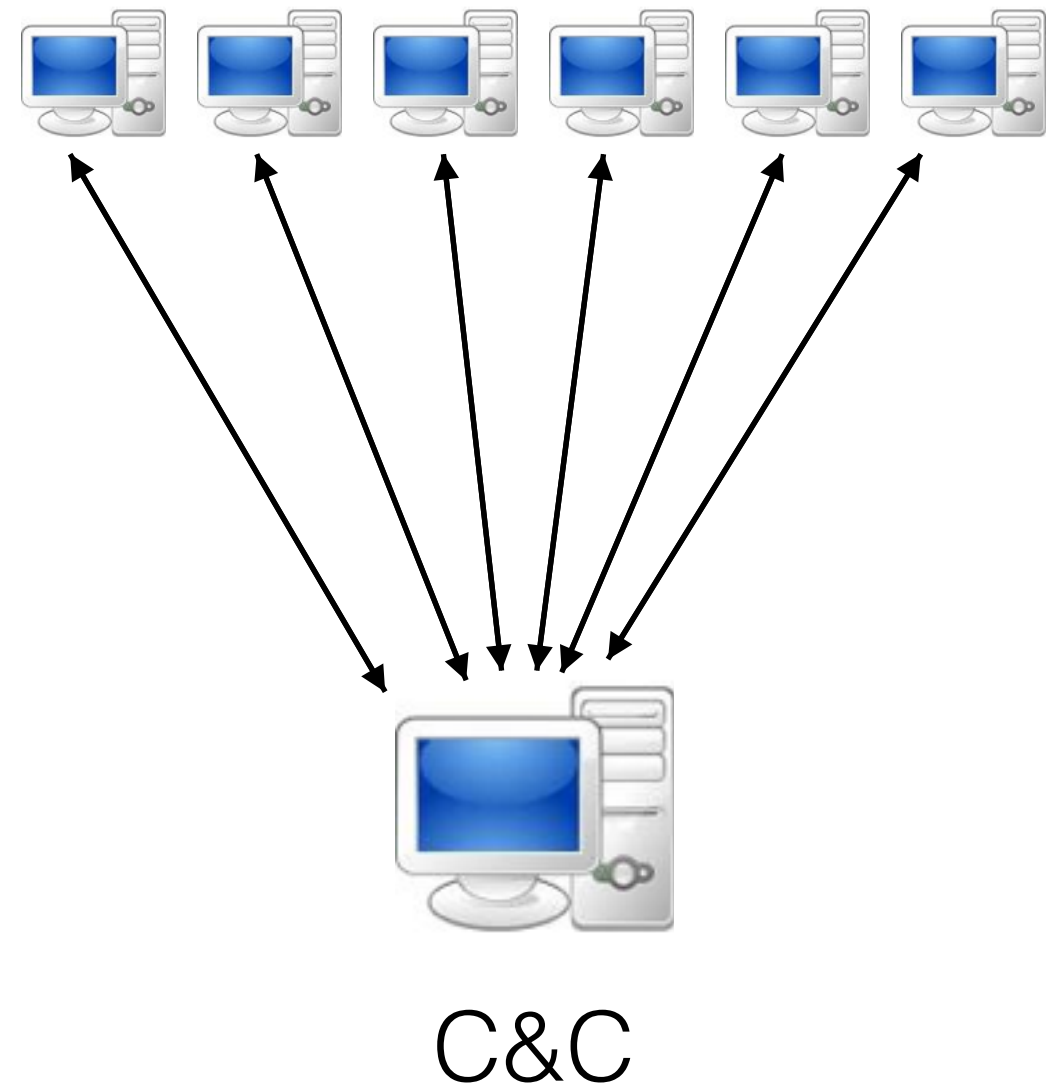


C&C



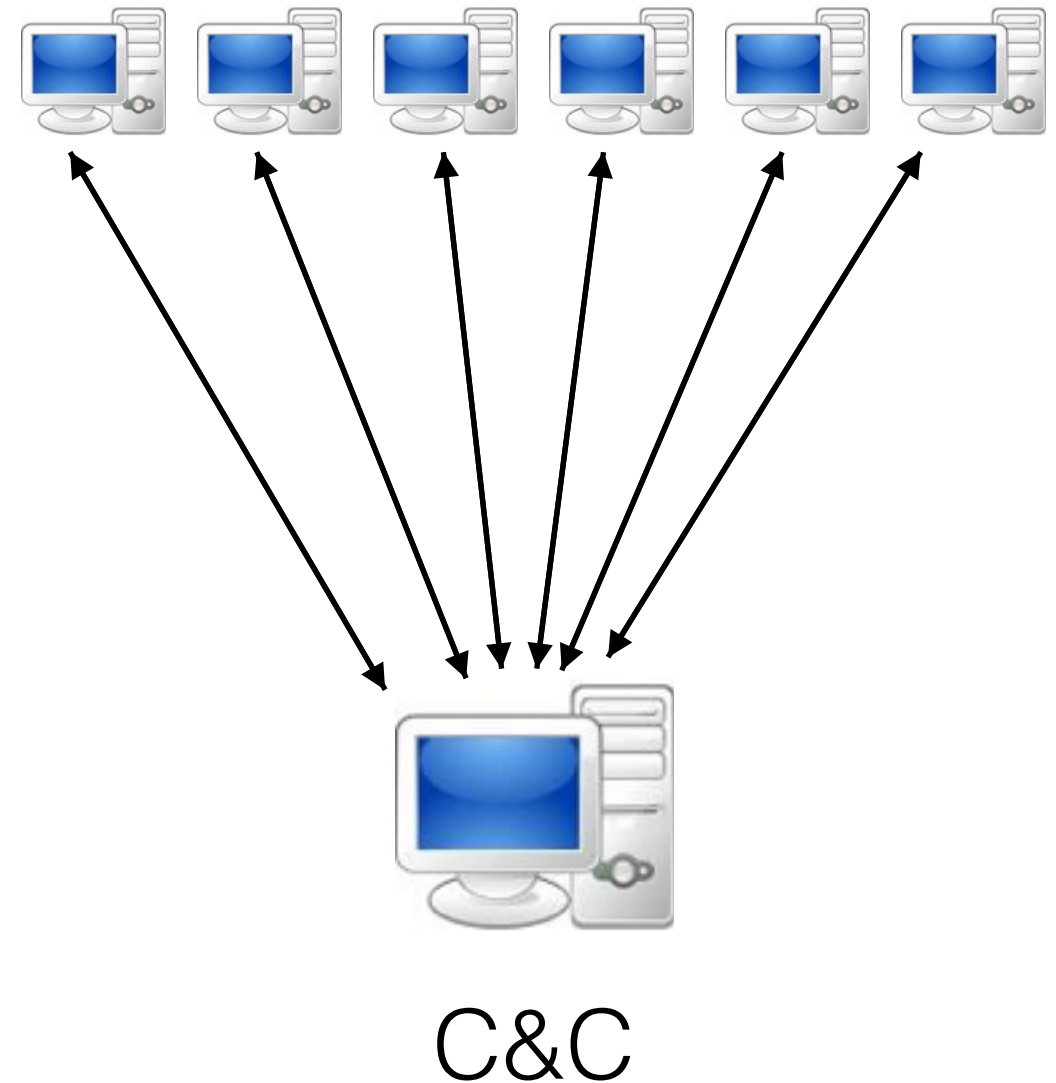
# Botnet

- Collection of compromised machines (bots) under unified control of an attacker (botmaster)
- Method of compromise decoupled from method of control
  - Launch a worm/virus, etc.: remember, payload is orthogonal!
- Upon infection, a new bot “phones home” to *rendezvous* with botnet “command-and-control” (C&C)
- Botmaster uses C&C to push out commands and updates



# Botnet

- Collection of compromised machines (bots) under unified control of an attacker (botmaster)
- Method of compromise decoupled from method of control
  - Launch a worm/virus, etc.: remember, payload is orthogonal!
- Upon infection, a new bot “phones home” to *rendezvous* with botnet “command-and-control” (C&C)
- Botmaster uses C&C to push out commands and updates



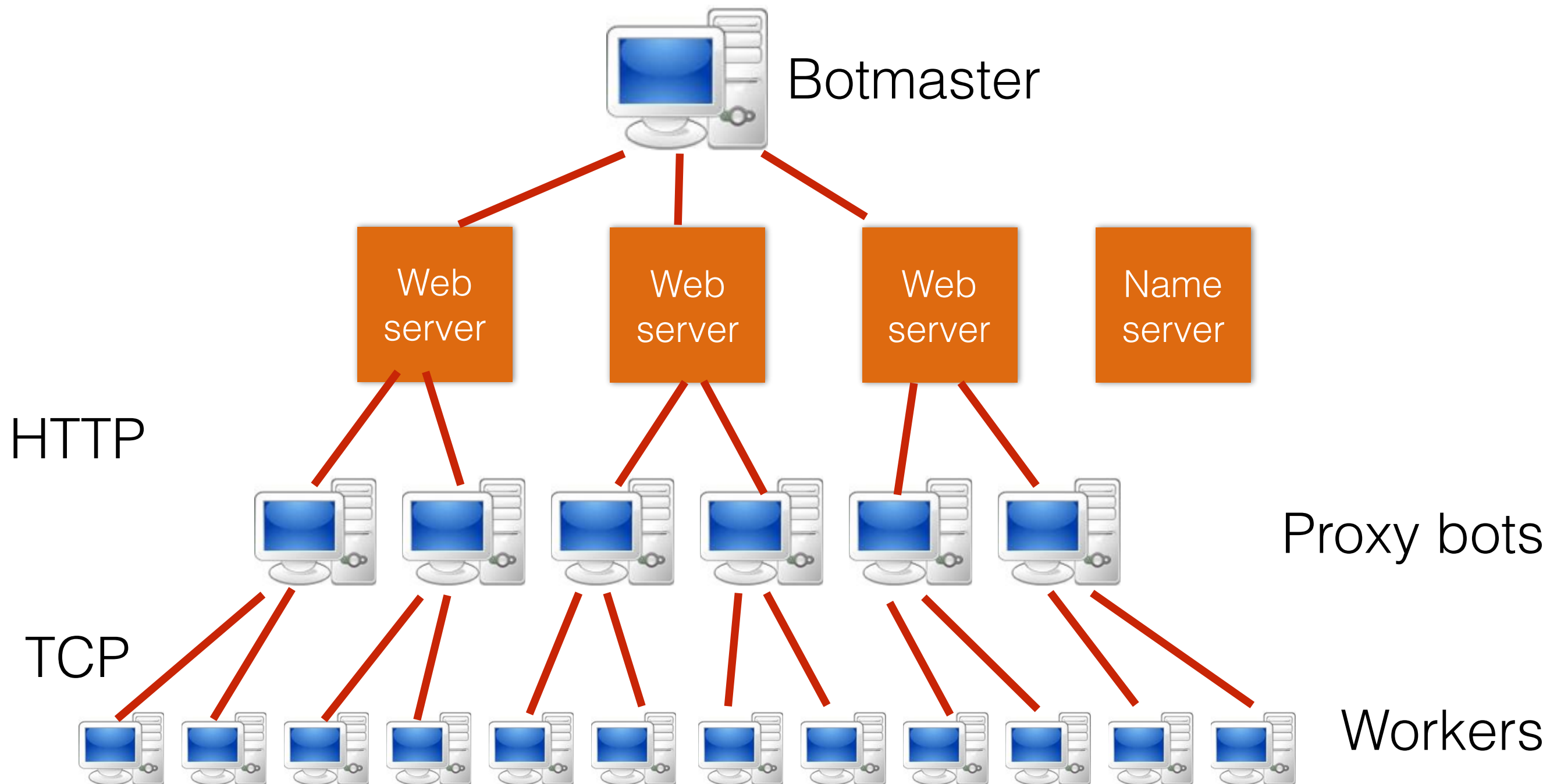
Topology can be star (like this), hierarchical, peer-to-peer...

# Supporting clicks

- Ideally a user will click on an embedded URL
- Result is more complex than just going to a web server
  - Defensive measures: URL and domain blacklisting & takedown notices by ISPs
- Confuse defenses (esp. blacklisting) with moving targets:
  - Redirection sites (legit-looking URL, like a URL shortener, or just manage DNS yourself and create throwaway domains that redirect to a more permanent domain)
  - Bulk domains: purchased from a reseller or as part of an affiliate program (more later)
- But web servers are static, so how do we keep them from being shut down due to blacklisting and takedown notices?

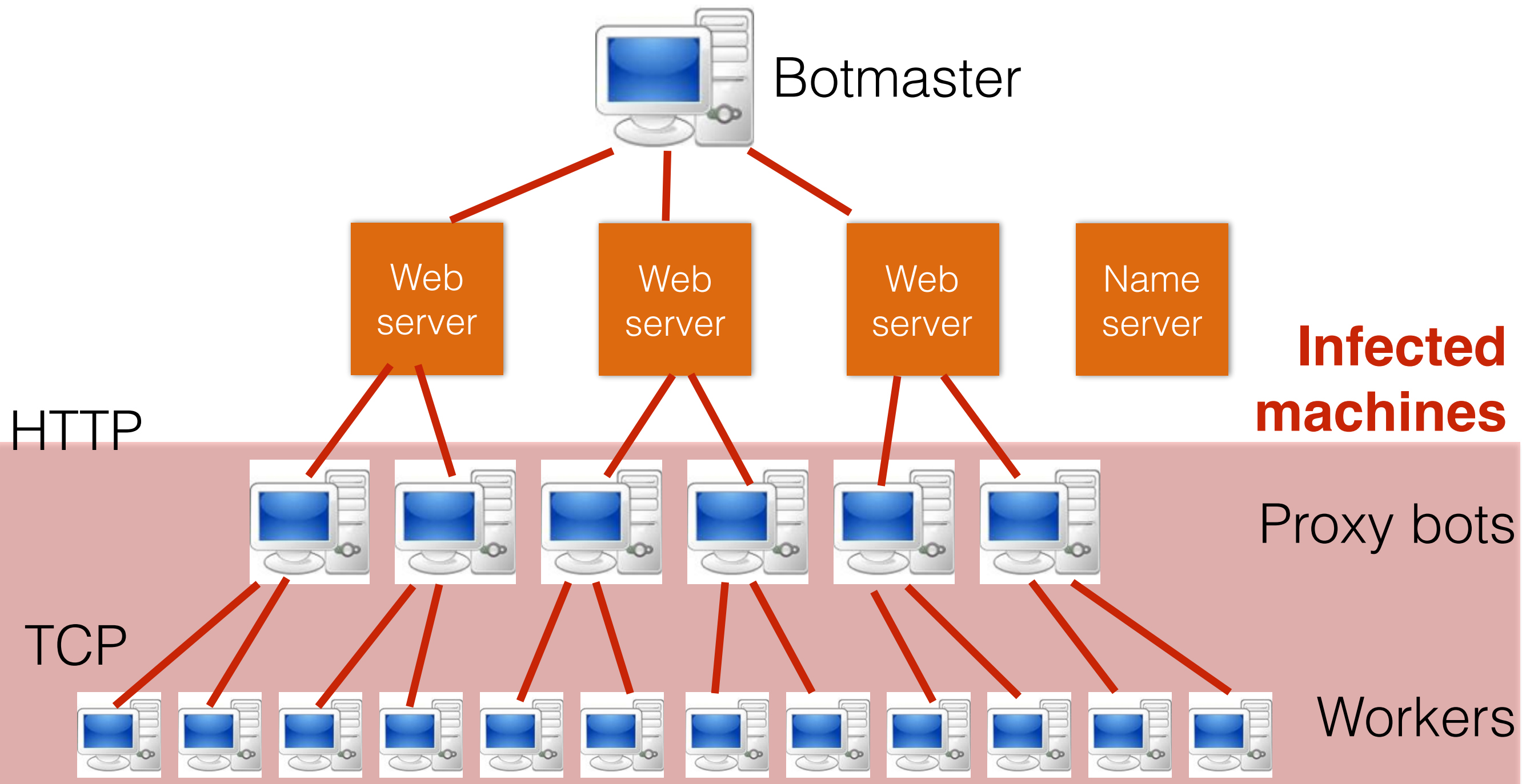
# Spambot

Botnet used for sending spam



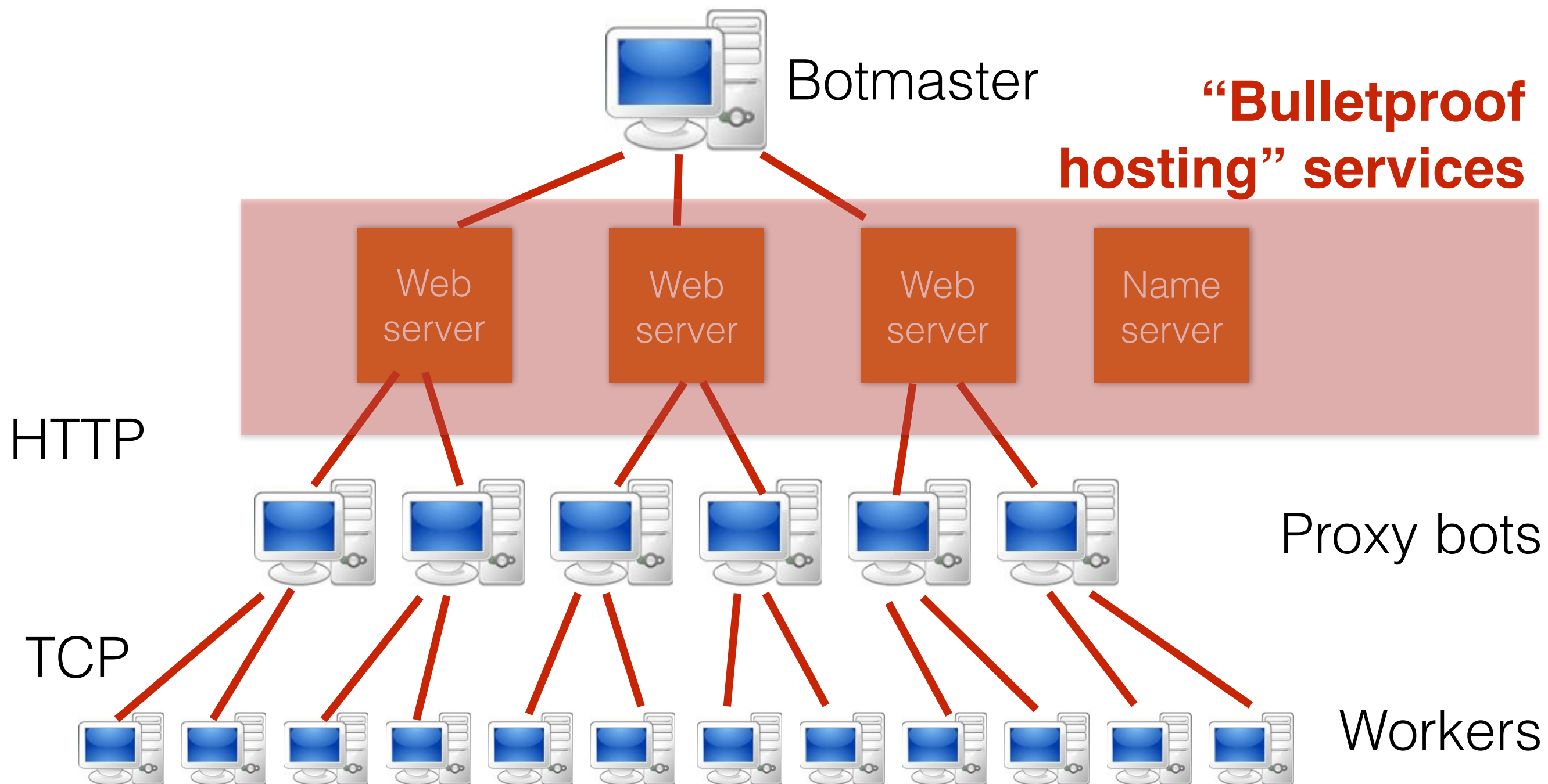
# Spambot

Botnet used for sending spam



# Spambot

Botnet used for sending spam



# Bulletproof hosting sites

- Services / specific hosts are often blocked by appealing to their ISPs (“please block this user..”)
- Bulletproof hosting services will refuse to block you (for a price)
- Many have been taken down
  - Often linked to criminal organizations
- Storm botnet: Controller likely run by Russian Business Network
  - Used Atrivo as their bulletproof hosting service

# Why multiple levels of indirection

- Many workers send email
- User clicks: gets sent to a proxy bot, who redirects to a web server
- Why proxies?
  - To subvert defenses that block IP addresses
  - Keep the IP address for a given host ([buydrugs.ru](http://buydrugs.ru)) moving
- “Fast flux” network
  - Short-lived TTLs in DNS responses (hostname to IP address mapping changes quickly)
  - Web proxies to a set of fixed web servers



Quick botnet aside...

# Monetizing botnets

- General malware monetization approaches apply:
  - Keyloggers (steal financial, email, social network, etc. accounts)
  - Ransomware
  - Transaction generators
    - Watch user's surfing
    - Wait to log into banking site and inject extra money, then alter web server replies to mask change in user balance
    - Or wait until the user clicks and inject your own, too.

# Monetizing botnets

- Additionally, botnets give you massive scale
  - DDoS
  - Click fraud
  - Scam infrastructure
    - Hosting web pages (e.g., for phishing)
    - Redirection to evade blacklisting/takedown notices
  - Spam

# Monetizing botnets

- Additionally, botnets give you massive scale
  - DDoS
  - Click fraud
  - Scam infrastructure
    - Hosting web pages (e.g., for phishing)
    - Redirection to evade blacklisting/takedown notices
  - Spam

**None of these cause serious pain for the infected user!**

**Users have little incentive to prevent these**

# Advertising your botnet

How do you advertise the capabilities of your amazing botnet?

# Advertising your botnet

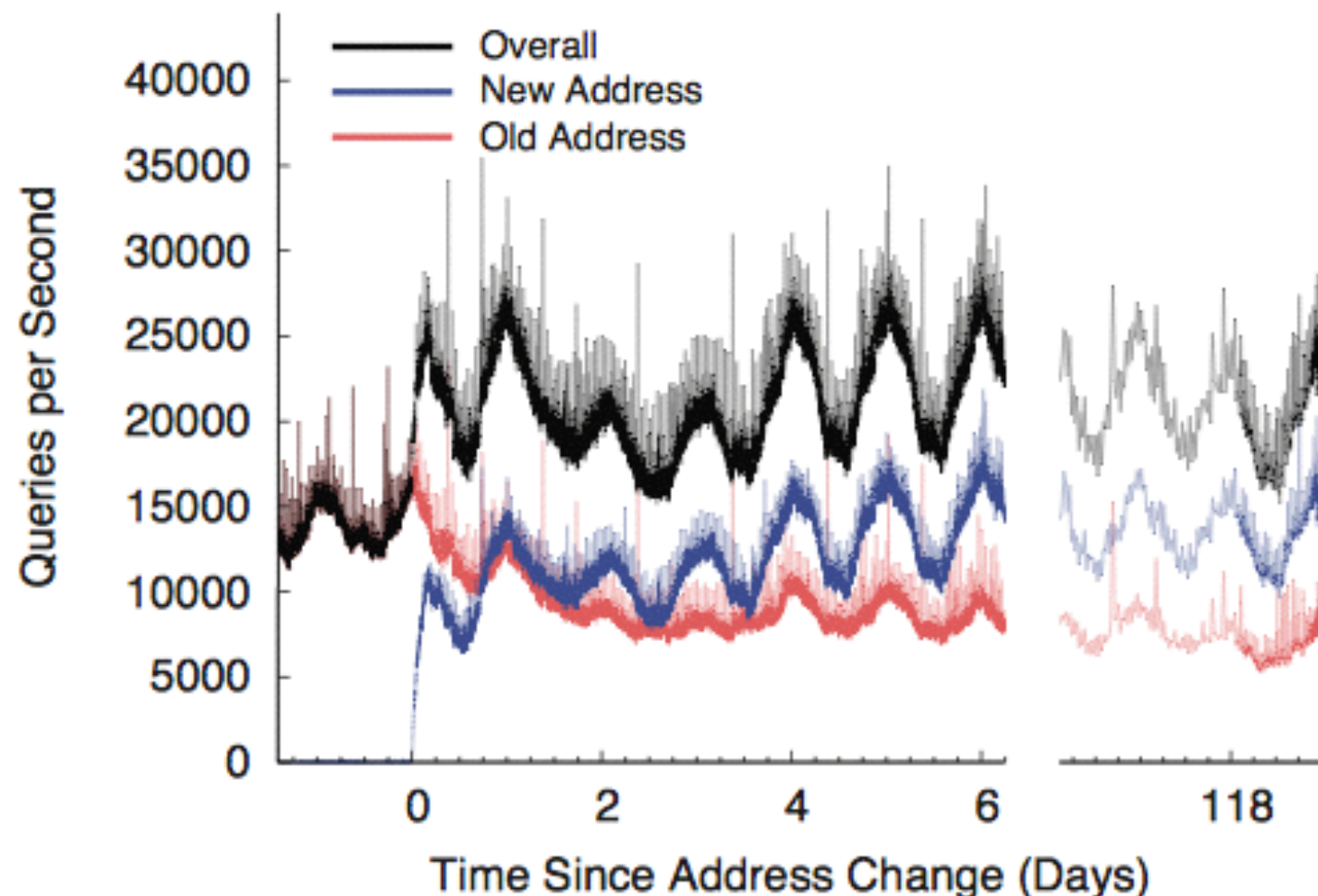
How do you advertise the capabilities of your amazing botnet?

Some DNS root servers advertise query volume  
“see how much attack traffic we can fend off!”

# Advertising your botnet

How do you advertise the capabilities of your amazing botnet?

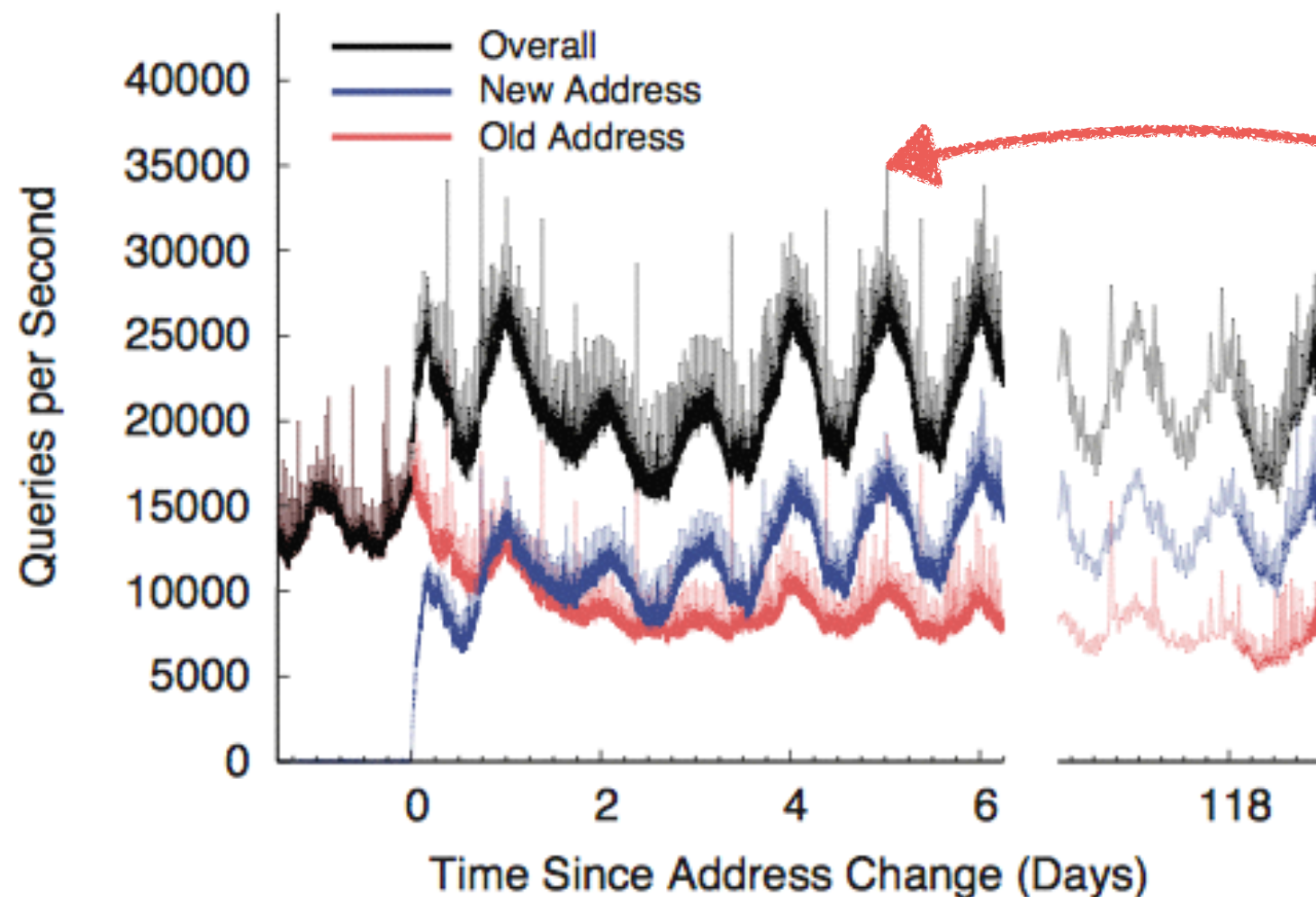
Some DNS root servers advertise query volume  
“see how much attack traffic we can fend off!”



# Advertising your botnet

How do you advertise the capabilities of your amazing botnet?

Some DNS root servers advertise query volume  
“see how much attack traffic we can fend off!”



“Look for the surge  
4 days from now”



# The importance of botnets

- Botnets represent the “great modern threat” of the Internet
- Why not worms?

# The importance of botnets

- Botnets represent the “great modern threat” of the Internet
- Why not worms?
  - Greater control over botnets
  - Less emergent
  - Quieter
  - Flexible

# Taking down botnets

# Taking down botnets

- Approach #1: **prevent** the initial bot infection
  - Infection is decoupled from bot's participation in the botnet, so this is equivalent to preventing malware infections in general - *hard*
- Approach #2: **Take down** the C&C master server
- Botmaster counter-measures?

# Taking down botnets

- Approach #1: **prevent** the initial bot infection
  - Infection is decoupled from bot's participation in the botnet, so this is equivalent to preventing malware infections in general - *hard*
- Approach #2: **Take down** the C&C master server
- Botmaster counter-measures?
  - Move the C&C around: each day (e.g.) bots generate a large list of possible domain names.
  - Try a random subset looking for C&C server.
  - Server signs its replies

# Taking down botnets

- Approach #1: **prevent** the initial bot infection
  - Infection is decoupled from bot's participation in the botnet, so this is equivalent to preventing malware infections in general - *hard*
- Approach #2: **Take down** the C&C master server
- Botmaster counter-measures?
  - Move the C&C around: each day (e.g.) bots generate a large list of possible domain names.
  - Try a random subset looking for C&C server.
  - Server signs its replies

**Counter-counter measure?**

...back to spam

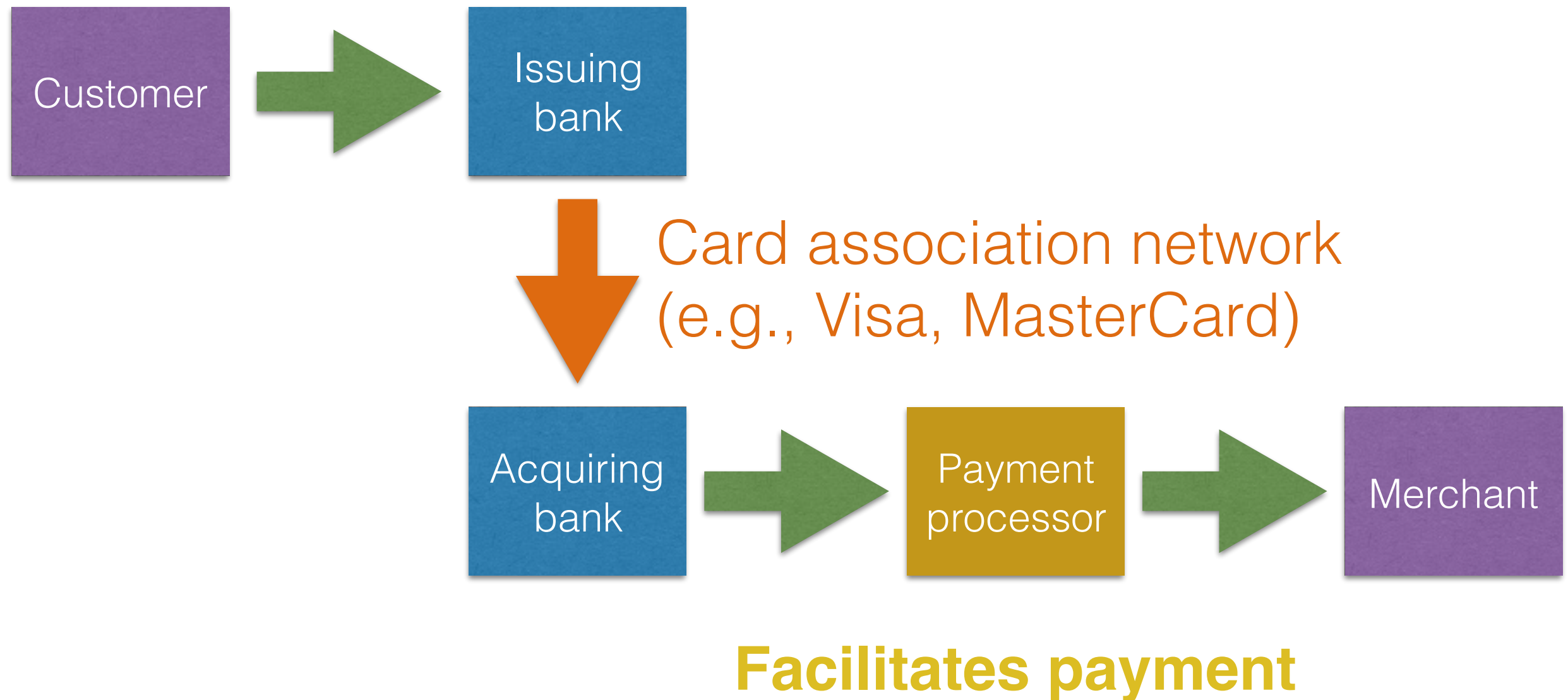
# Affiliate programs

Markets drive efficiency and specialization:  
some specialize in botnets, others in spam

- You can join an affiliate program!
  - You send out emails and get a commission (30–50%)
- Affiliate program provides:
  - Storefront templates, shopping cart management
  - Analytics support
  - Advertising materials
  - Central web service interface for affiliates to track conversions and to register for payouts
  - Domains bought in bulk
  - ...



# Realization: Getting paid



# Realization: Shipping goods

- Business-to-business websites will make connections across many different goods
  - Alibaba, EC-Plaza, ECTrade, ...
- Commonly offer “drop shipping”
  - The spambot operator does not need to purchase any warehouse/storage

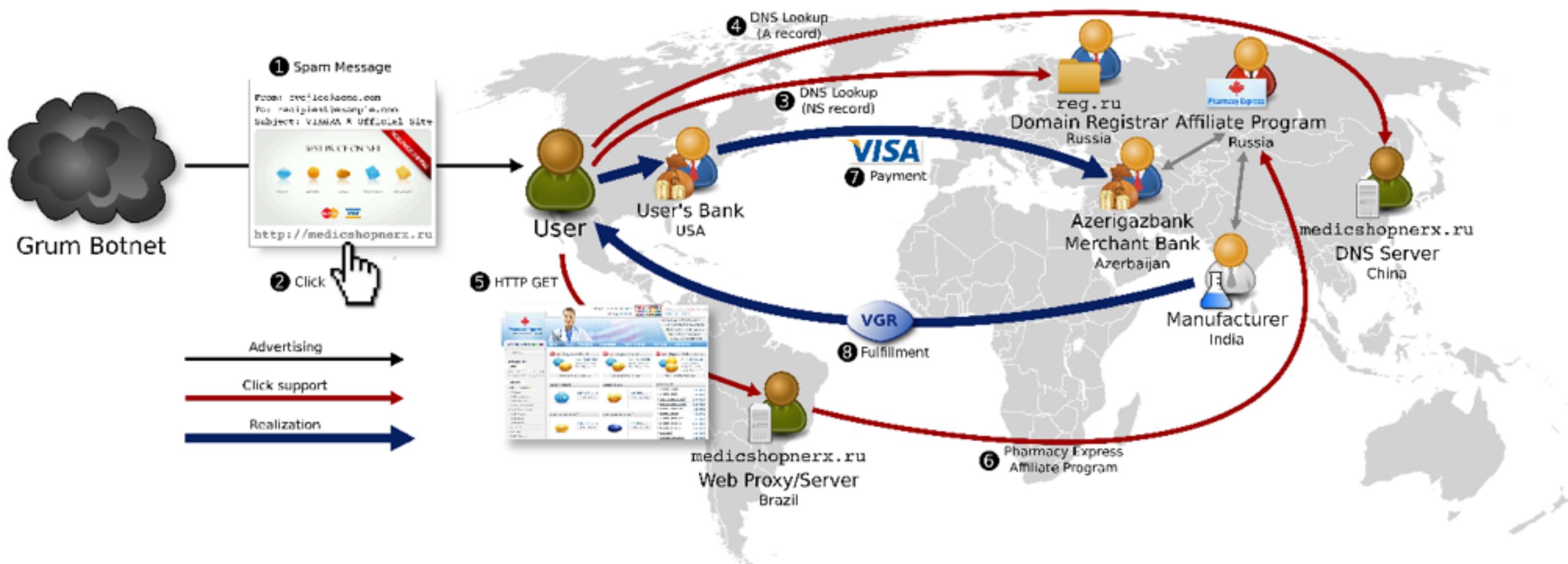


Figure 1: Infrastructure involved in a single URL's value chain, including advertisement, click support and realization steps.

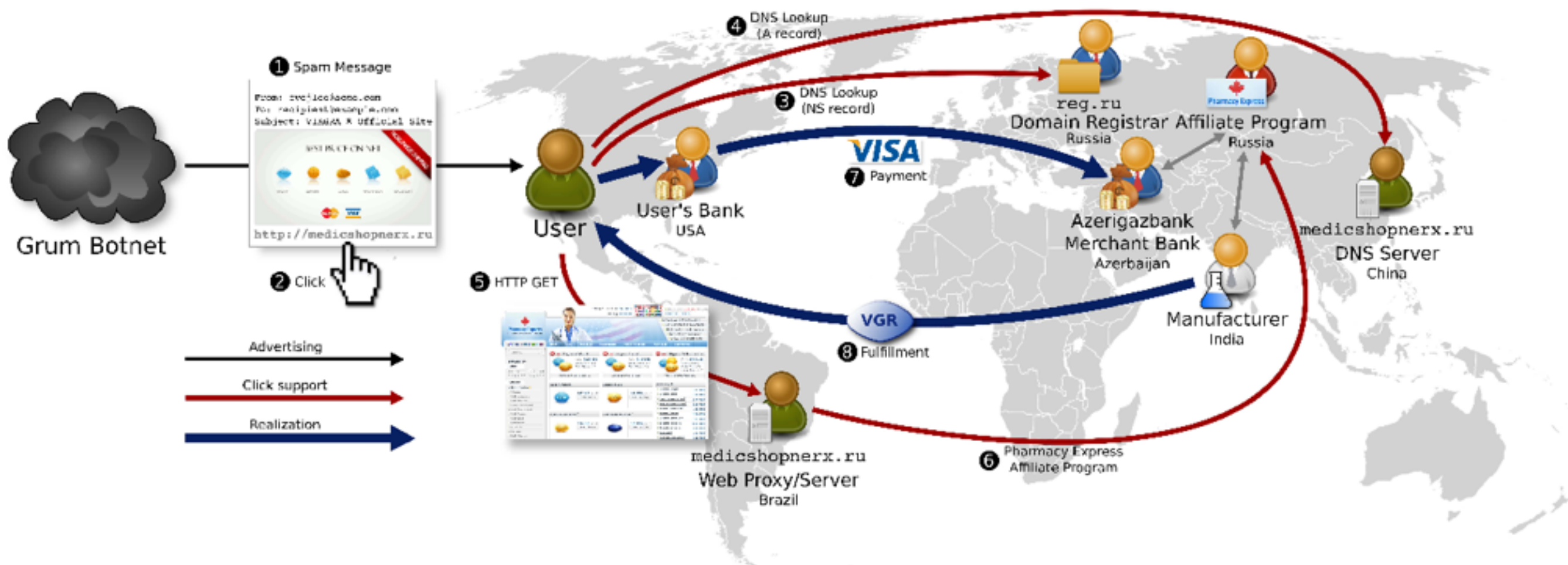


Figure 1: Infrastructure involved in a single URL's value chain, including advertisement, click support and realization steps.

1. Spam delivered

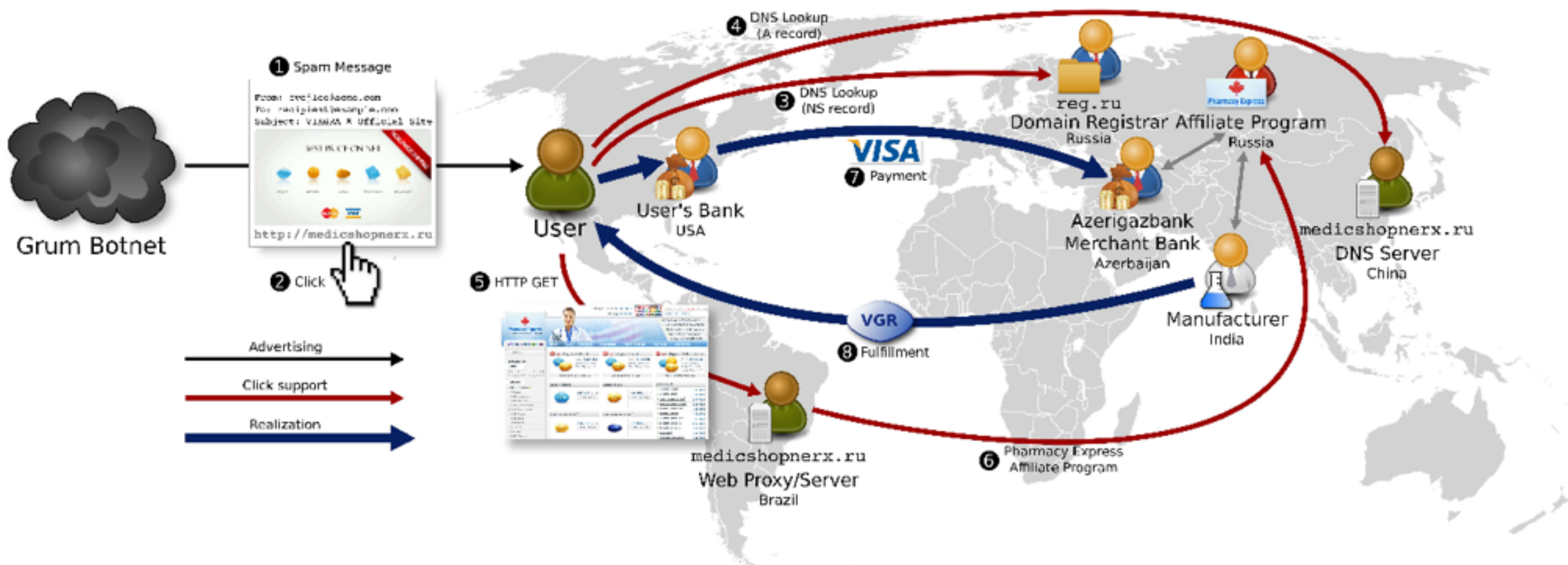


Figure 1: Infrastructure involved in a single URL's value chain, including advertisement, click support and realization steps.

1. Spam delivered
2. User clicks



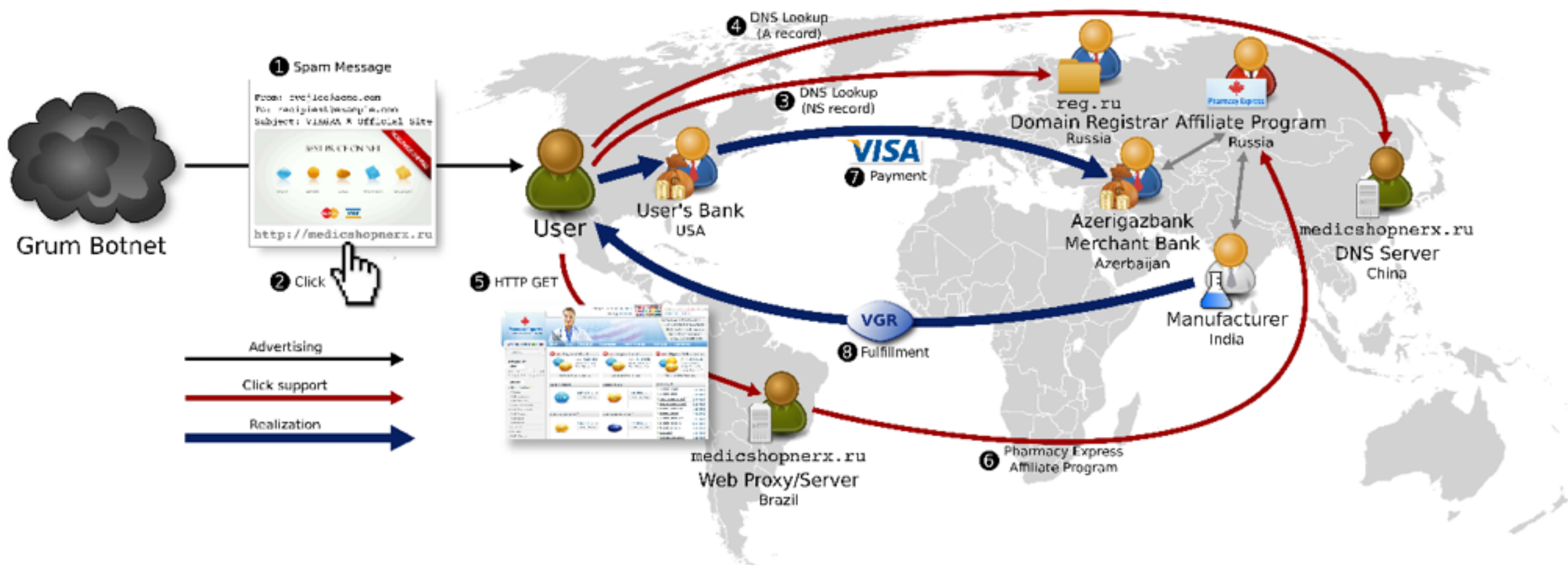


Figure 1: Infrastructure involved in a single URL's value chain, including advertisement, click support and realization steps.

1. Spam delivered
2. User clicks
3. Domain registered by `reg.ru`

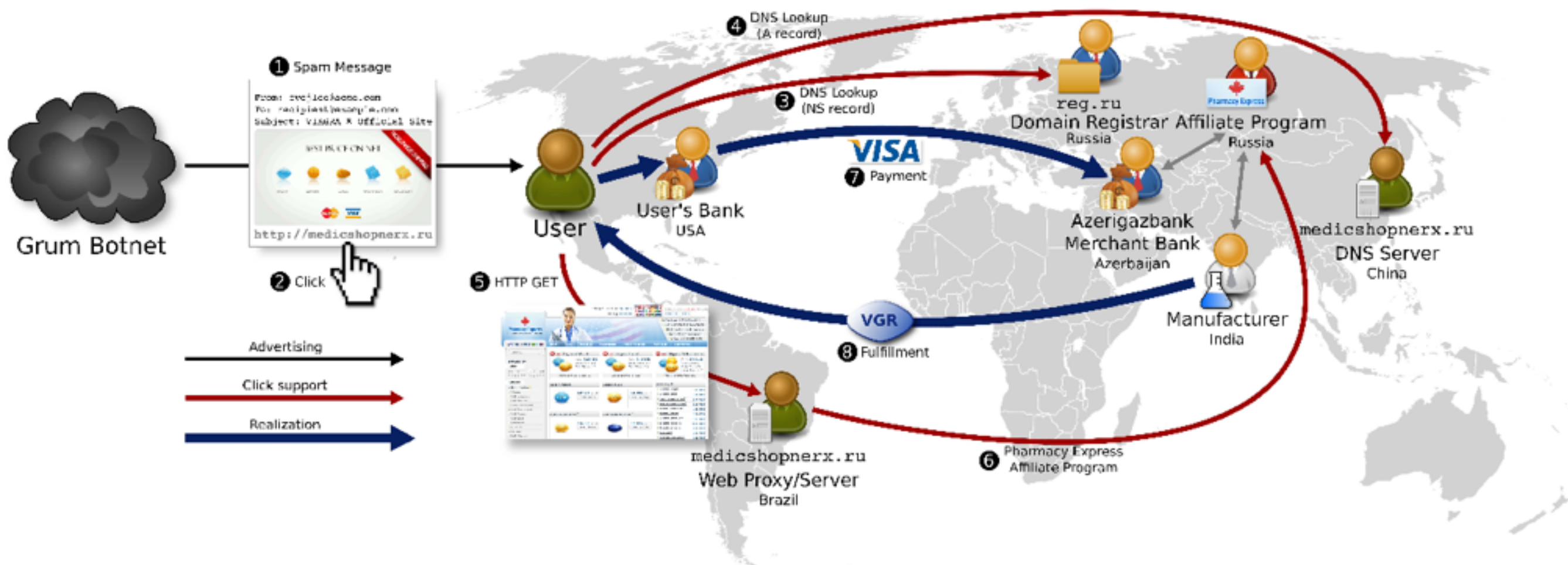


Figure 1: Infrastructure involved in a single URL's value chain, including advertisement, click support and realization steps.

1. Spam delivered
2. User clicks
3. Domain registered by `reg.ru`
4. Nameserver hosted in China

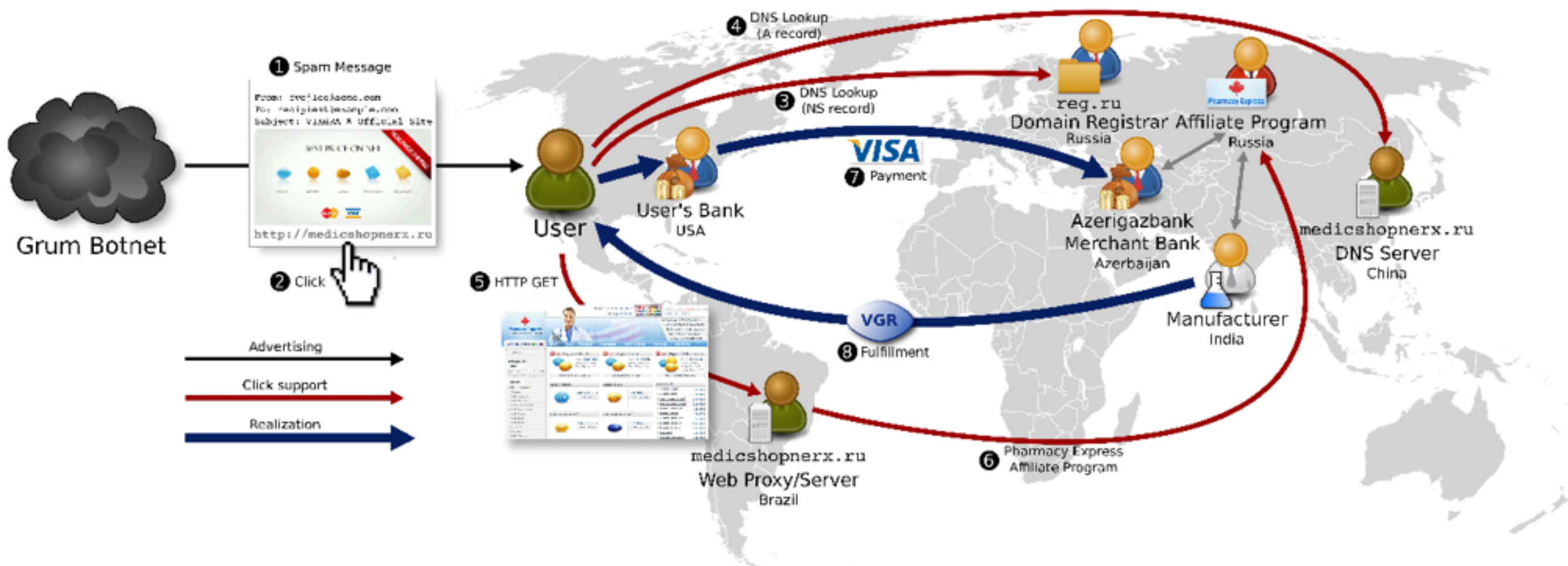


Figure 1: Infrastructure involved in a single URL's value chain, including advertisement, click support and realization steps.

1. Spam delivered
2. User clicks
3. Domain registered by `reg.ru`
4. Nameserver hosted in China
5. Renders storefront



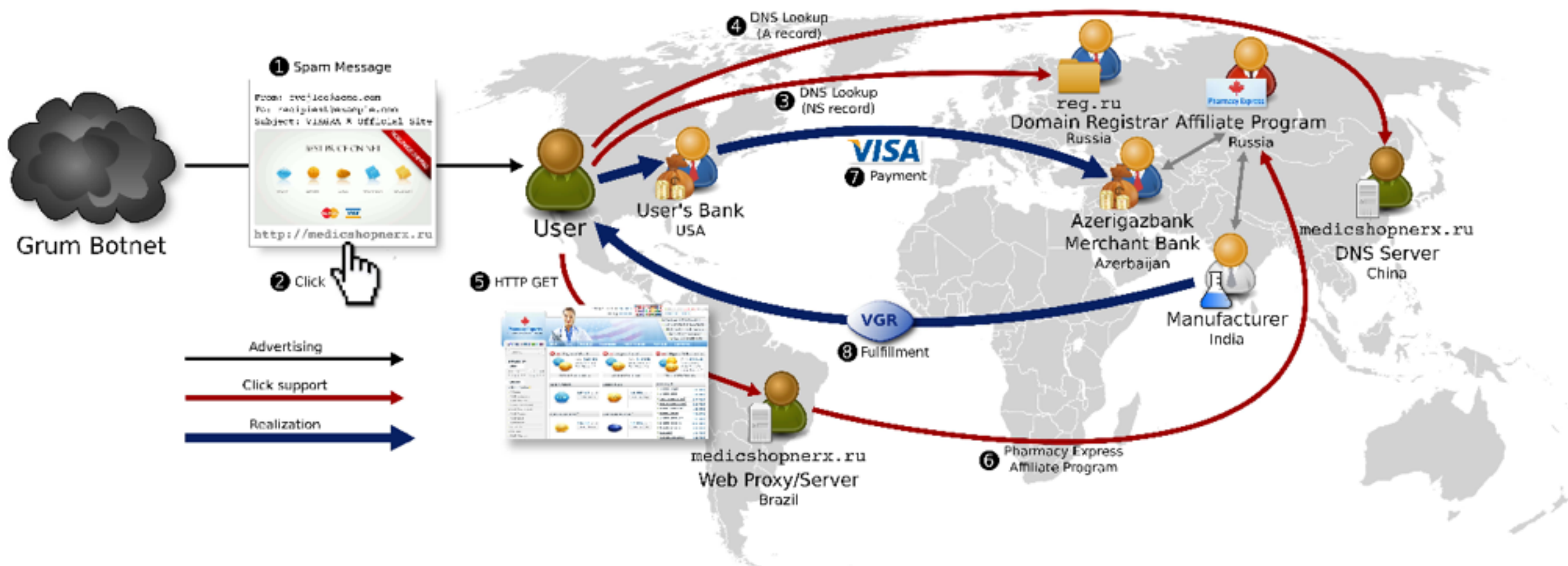


Figure 1: Infrastructure involved in a single URL's value chain, including advertisement, click support and realization steps.

1. Spam delivered
2. User clicks
3. Domain registered by `reg.ru`
4. Nameserver hosted in China
5. Renders storefront
6. Analytics updated at affiliate

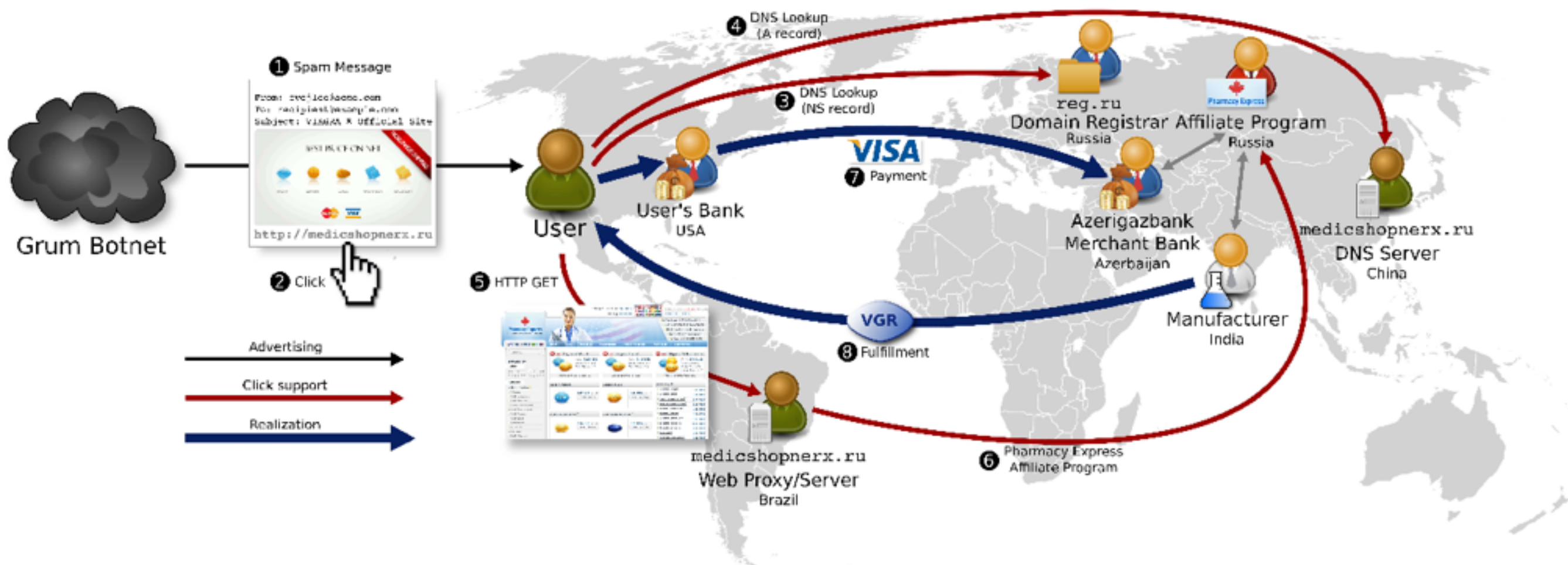


Figure 1: Infrastructure involved in a single URL's value chain, including advertisement, click support and realization steps.

1. Spam delivered
2. User clicks
3. Domain registered by `reg.ru`
4. Nameserver hosted in China
5. Renders storefront
6. Analytics updated at affiliate
7. User makes payment; acquiring bank in Azerbaijan

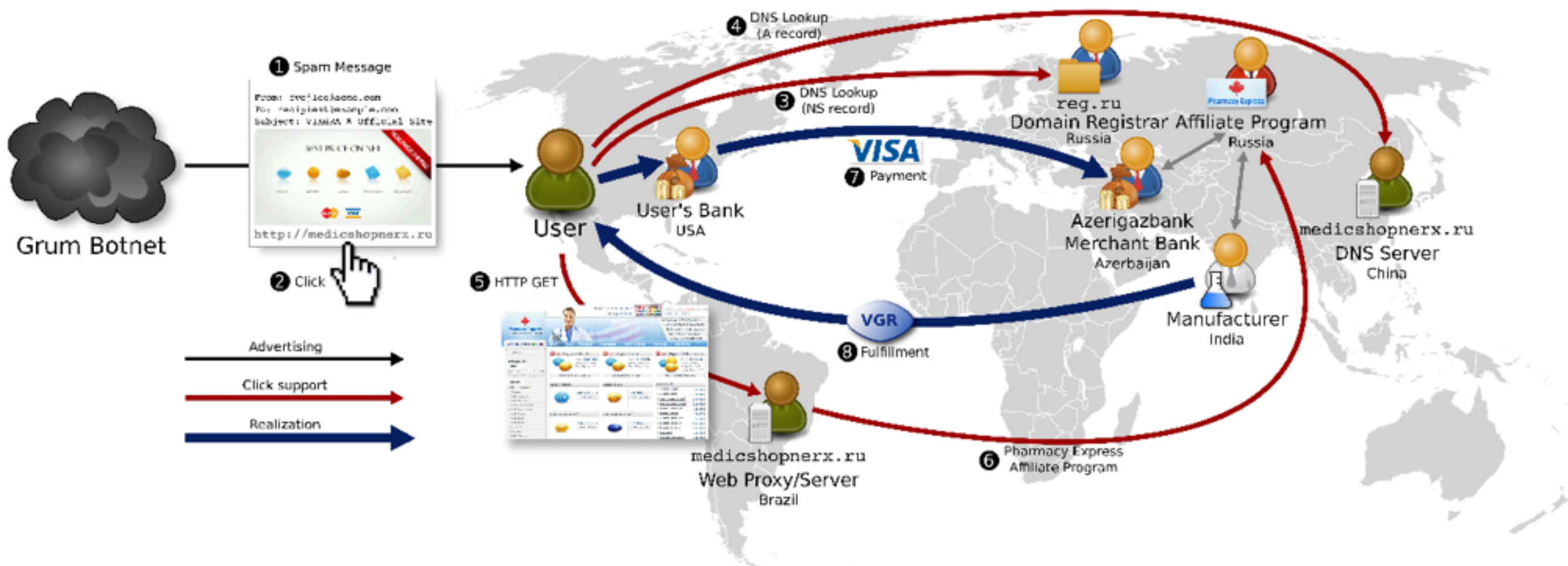


Figure 1: Infrastructure involved in a single URL's value chain, including advertisement, click support and realization steps.

1. Spam delivered
2. User clicks
3. Domain registered by `reg.ru`
4. Nameserver hosted in China
5. Renders storefront
6. Analytics updated at affiliate
7. User makes payment; acquiring bank in Azerbaijan
8. Supplier in Chennai, India delivers 10 days later



# Analyzing spam “click trajectories”

Measurement study  
out of UCSD

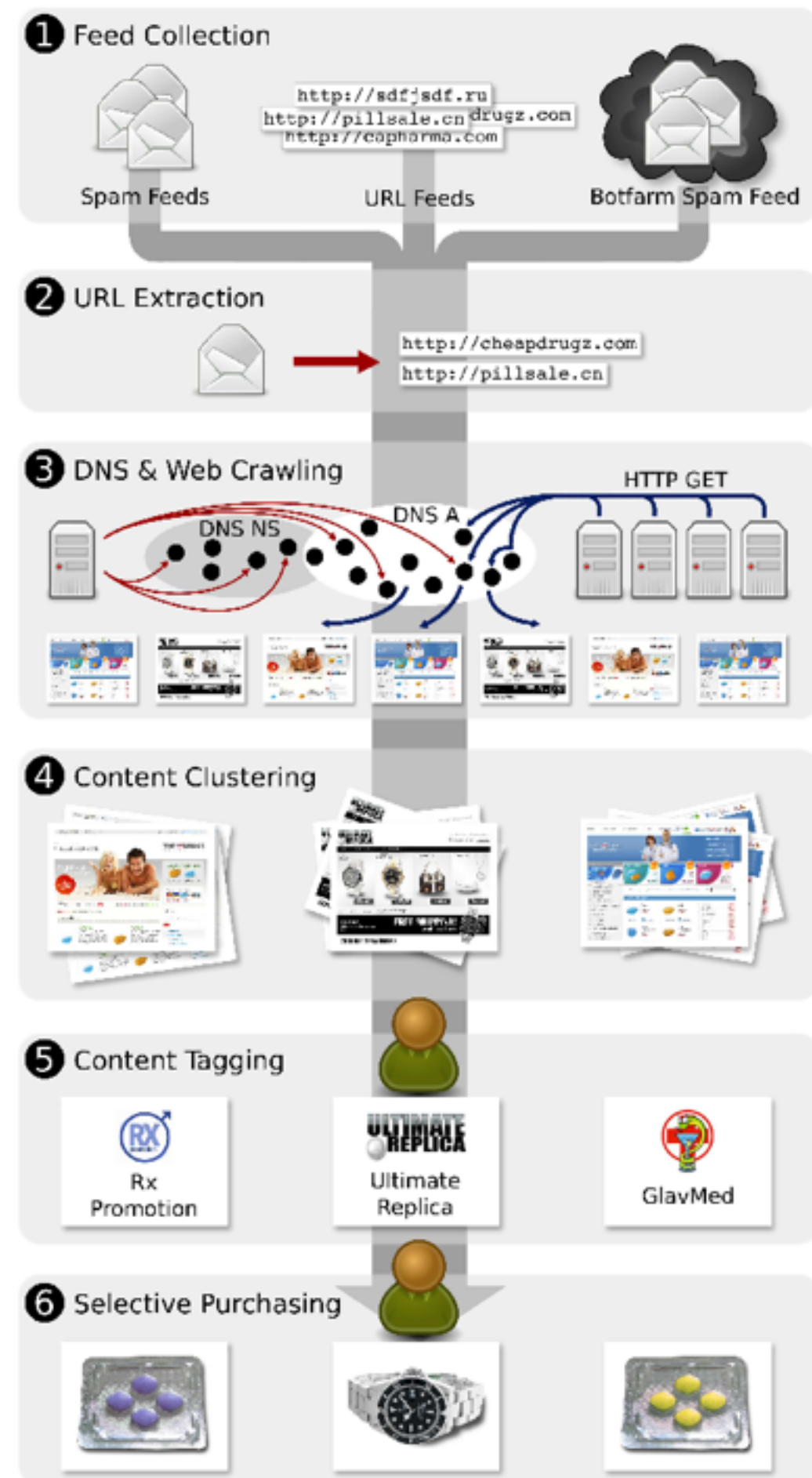


Figure 2: Our data collection and processing workflow.

# Who/what gets sold

- Three most common products sold:
  - Pharmaceuticals (vast majority)
  - Replica luxury goods
  - Counterfeit software
- Run by relatively few affiliate programs

<i>Stage</i>	<i>Pharmacy</i>	<i>Software</i>	<i>Replicas</i>	<i>Total</i>
URLs	346,993,046	3,071,828	15,330,404	365,395,278
Domains	54,220	7,252	7,530	69,002
Web clusters	968	51	20	1,039
Programs	30	5	10	45

Table III: Breakdown of clustering and tagging results.

Few affiliate programs constitute the majority

<i>Affiliate Program</i>		<i>Distinct Domains</i>	<i>Received URLs</i>	<i>Feed Volume</i>
RxPrm	RX–Promotion	10,585	160,521,810	24.92%
Mailn	Mailien	14,444	69,961,207	23.49%
PhEx	Pharmacy Express	14,381	69,959,629	23.48%
EDEx	ED Express	63	1,578	0.01%
ZCashPh	ZedCash (Pharma)	6,976	42,282,943	14.54%
DrMax	Dr. Maxman	5,641	32,184,860	10.95%
Grow	Viagrow	382	5,210,668	1.68%
USHC	US HealthCare	167	3,196,538	1.31%
MaxGm	MaxGentleman	672	1,144,703	0.41%
VgREX	VigREX	39	426,873	0.14%
Stud	Stud Extreme	42	68,907	0.03%
ManXt	ManXtenz	33	50,394	0.02%
GlvMd	GlavMed	2,933	28,313,136	10.32%
OLPh	Online Pharmacy	2,894	17,226,271	5.16%
Eva	EvaPharmacy	11,281	12,795,646	8.7%
WldPh	World Pharmacy	691	10,412,850	3.55%



# What gets sold

<i>Supplier</i>	<i>Item</i>	<i>Origin</i>	<i>Affiliate Programs</i>
Aracoma Drug	Orange bottle of tablets (pharma)	WV, USA	ClFr
Combitic Global Caplet Pvt. Ltd.	Blister-packed tablets (pharma)	Delhi, India	GlvMd
M.K. Choudhary	Blister-packed tablets (pharma)	Thane, India	OLPh
PPW	Blister-packed tablets (pharma)	Chennai, India	PhEx, Stmul, Trust, ClFr
K. Sekar	Blister-packed tablets (pharma)	Villupuram, India	WldPh
Rhine Inc.	Blister-packed tablets (pharma)	Thane, India	RxPrm, DrgRev
Supreme Suppliers	Blister-packed tablets (pharma)	Mumbai, India	Eva
Chen Hua	Small white plastic bottles (herbal)	Jiangmen, China	Stud
Etech Media Ltd	Novelty-sized supplement (herbal)	Christchurch, NZ	Staln
Herbal Health Fulfillment Warehouse	White plastic bottle (herbal)	MA, USA	Eva
MK Sales	White plastic bottle (herbal)	WA, USA	GlvMd
Riverton, Utah shipper	White plastic bottle (herbal)	UT, USA	DrMax, Grow
Guo Zhonglei	Foam-wrapped replica watch	Baoding, China	Dstn, UltRp

Table VI: List of product suppliers and associated affiliate programs and/or store brands.

# Acquiring banks

<i>Bank Name</i>	<i>BIN</i>	<i>Country</i>	<i>Affiliate Programs</i>
Azerigazbank	404610	Azerbaijan	GlvMd, RxPrm, PhEx, Stmul, RxPnr, WldPh
B&N	425175	Russia	ASR
B&S Card Service	490763	Germany	MaxGm
Borgun Hf	423262	Iceland	Trust
Canadian Imperial Bank of Commerce	452551	Canada	WldPh
Cartu Bank	478765	Georgia	DrgRev
DnB Nord (Pirma)	492175	Latvia	Eva, OLPh, USHC
Latvia Savings	490849	Latvia	EuSft, OEM, WchSh, Royal, SftSl
Latvijas Pasta Banka	489431	Latvia	SftSl
St. Kitts & Nevis Anguilla National Bank	427852	St. Kitts & Nevis	DmdRp, VgREX, Dstn, Luxry, SwsRp, OneRp
State Bank of Mauritius	474140	Mauritius	DrgRev
Visa Iceland	450744	Iceland	Staln
Wells Fargo	449215	USA	Green
Wirecard AG	424500	Germany	ClFr

Table V: Merchant banks authorizing or settling transactions for spam-advertised purchases, their Visa-assigned Bank Identification Number (BIN), their location, and the abbreviation used in Table IV for affiliate program and/or store brand.



# So how much are spambots making?

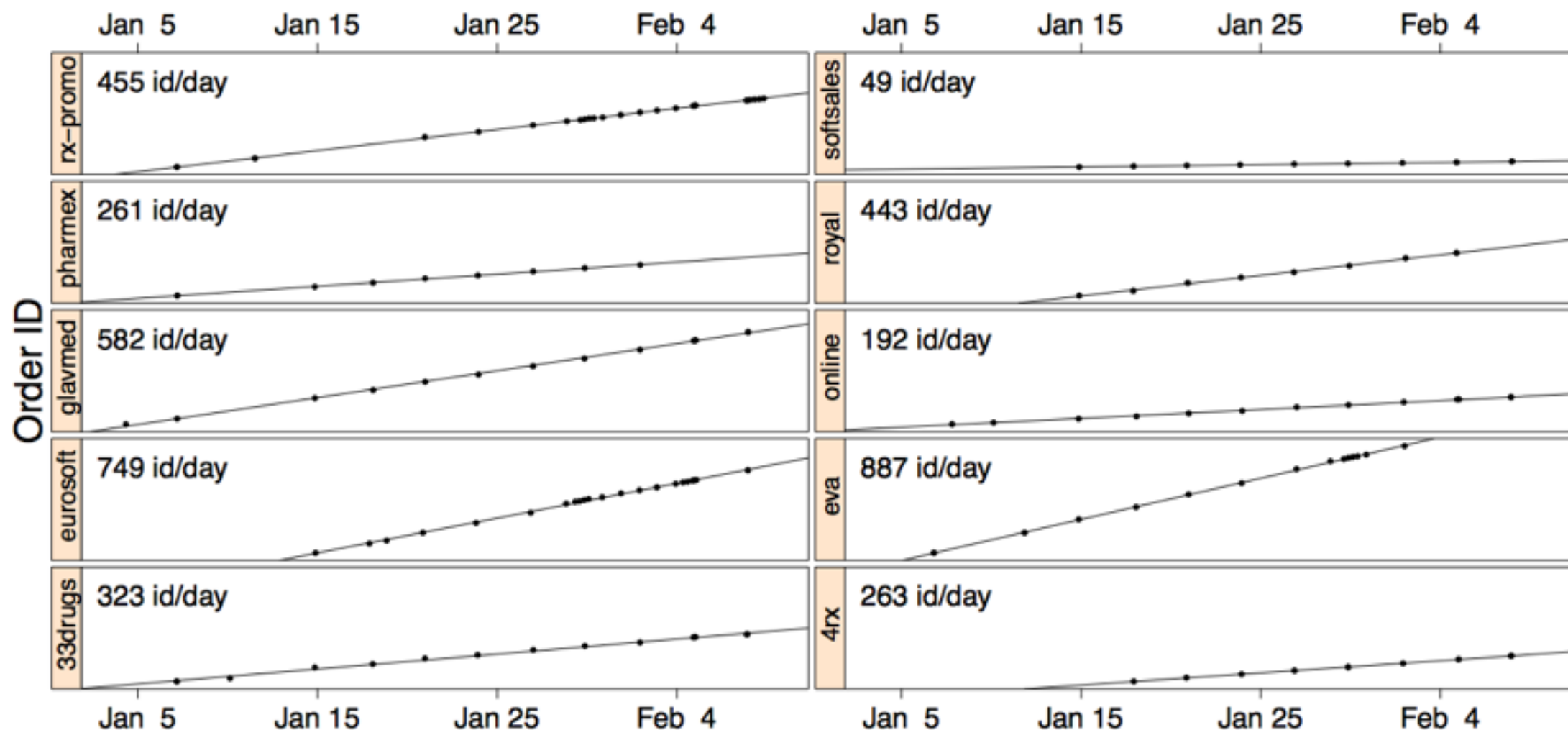
- To understand, we would have to know:
  - Order volume (how much is sold as a result of an affiliate program over time?)
  - Purchasing behavior (what are people buying?)
- Turns out you can infer these

# Predicting order volume

- Most affiliate programs provide a confirmation page with an order number
- This order number usually just increments

# Predicting order volume

- Most affiliate programs provide a confirmation page with an order number
- This order number usually just increments



# Inferring what people buy

- EvaPharmacy (a top 5 spam-advertised pharmacy affiliate program):
  - 2/3 of outsourced image hosting was to compromised 3rd party servers
- They contacted the owners of these servers and asked for logs
- Correlated image logs with purchases

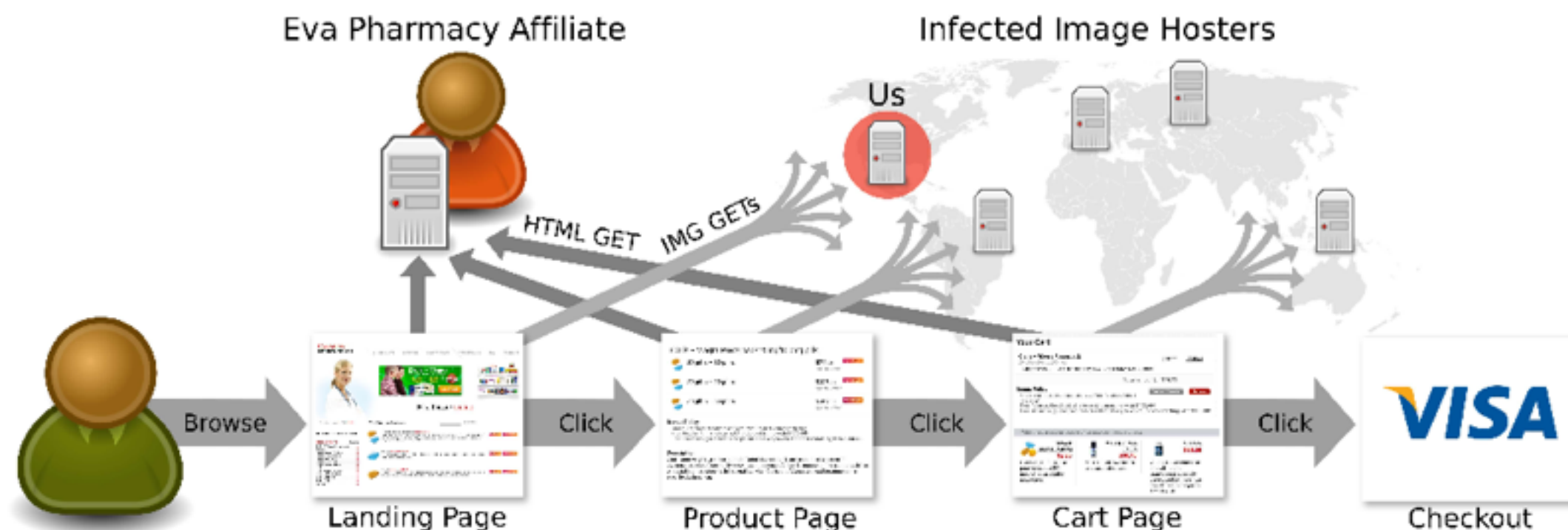


Figure 5: How a user interacts with an EvaPharmacy Web site, beginning with the landing page and then proceeding to a product page and the shopping cart. The main Web site contains embedded images hosted on separate compromised systems. When a browser visits such pages, the referrer information is sent to the image hosting servers for every new image visited.

# Affiliate profit

Affiliate Program	orders/month	<i>Spamalytics</i>		Min product price		Basket-weighted average	
		single order	rev/month	single order	rev/month	single order	rev/month
33drugs	9,862	\$100	\$980,000	\$45.00	\$440,000	\$57.25	\$560,000
4RX	8,001	\$100	\$800,000	\$34.50	\$280,000	\$95.00	\$760,000
EuroSoft	22,776	N/A	N/A	\$26.50	\$600,000	\$84.50	\$1,900,000
EvaPharmacy	26,962	\$100	\$2,700,000	\$50.50	\$1,300,000	\$90.00	\$2,400,000
GlavMed	17,933	\$100	\$1,800,000	\$54.00	\$970,000	\$57.00	\$1,000,000
Online Pharmacy	5,856	\$100	\$590,000	\$37.00	\$220,000	\$58.00	\$340,000
Pharmacy Express	7,933	\$100	\$790,000	\$51.00	\$410,000	\$58.75	\$460,000
Royal Software	13,483	N/A	N/A	\$55.25	\$750,000	\$133.75	\$1,800,000
Rx-Promotion	6,924	\$100	\$690,000	\$45.00	\$310,000	\$57.25	\$400,000
SoftSales	1,491	N/A	N/A	\$20.00	\$30,000	\$134.50	\$200,000

Table 4: Estimated monthly order volume, average purchase price, and monthly revenue (in dollars) per affiliate program using three different per-order price approximations.

Over 100k orders/month  
in this dataset alone

Some have guessed that  
“spammers make little  
money at all”

So who's  
actually buying  
this junk?



# So who's actually buying this junk?



Figure 6: The geographic distribution of those who added an item to their shopping cart.

Country	Visits	Cart Additions	Added Product
United States	517,793	3,707	0.72%
Canada	50,234	218	0.43%
Philippines	42,441	39	0.09%
United Kingdom	39,087	131	0.34%
Spain	26,968	59	0.22%
Malaysia	26,661	31	0.12%
France	18,541	37	0.20%
Germany	15,726	56	0.36%
Australia	15,101	86	0.57%
India	10,835	17	0.16%
China	8,924	30	0.34%
Netherlands	8,363	21	0.25%
Saudi Arabia	8,266	36	0.44%
Mexico	7,775	17	0.22%
Singapore	7,586	17	0.22%

Table 2: The top 15 countries and the percentage of visitors who added an item to their shopping cart.



So who's  
actually buying  
this junk?



Figure 6: The geographic distribution of those who added an item to their shopping cart.

Stop buying  
this junk!

Country	Visits	Cart Additions	Added Product
United States	517,793	3,707	0.72%
Canada	50,234	218	0.43%
Philippines	42,441	39	0.09%
United Kingdom	39,087	131	0.34%
Spain	26,968	59	0.22%
Malaysia	26,661	31	0.12%
France	18,541	37	0.20%
Germany	15,726	56	0.36%
Australia	15,101	86	0.57%
India	10,835	17	0.16%
China	8,924	30	0.34%
Netherlands	8,363	21	0.25%
Saudi Arabia	8,266	36	0.44%
Mexico	7,775	17	0.22%
Singapore	7,586	17	0.22%

Table 2: The top 15 countries and the percentage of visitors who added an item to their shopping cart.

# What are you buying?

Product	Quantity	Min order
Generic Viagra	568	\$78.80
Cialis	286	\$78.00
Cialis/Viagra Combo Pack	172	\$74.95
Viagra Super Active+	121	\$134.80
Female (pink) Viagra	119	\$44.00
Human Growth Hormone	104	\$83.95
Soma (Carisoprodol)	99	\$94.80
Viagra Professional	87	\$139.80
Levitra	83	\$100.80
Viagra Super Force	81	\$88.80
Cialis Super Active+	72	\$172.80
Amoxicillin	47	\$35.40
Lipitor	38	\$14.40
Ultram	38	\$45.60
Tramadol	36	\$82.80
Prozac	35	\$19.50
Cialis Professional	33	\$176.00
Retin A	31	\$47.85

**“Why do you rob banks?”**

**“Because that’s where the money is”**

*Why does the emergence of the underground economy matter?*

- Many of the centralized components of these networks get pursued and shut down
- Markets lead to efficiencies and specializations
  - Lowers barrier to entry: only need a single skill
  - Some underground market activities are legal
- Competition spurs innovation
  - Accelerates the arms race
  - Defenders must assume a more pessimistic threat model
- Facilitates non-\$ Internet attacks
  - Provides actors (political, nation-state) with cheap attack components

# Why studying it matters

*And why continuing to study it matters*

- Like any complex system, these markets can themselves be infiltrated
  - Some research on infiltrating affiliate programs & botnets, taking over C&C
- Can identify choke points
  - Many hosting services have been shut down
  - Draws attention to shady banks
  - Draws attention to shady doctors
    - Early spambot had one doctor writing 1500+ prescriptions per day