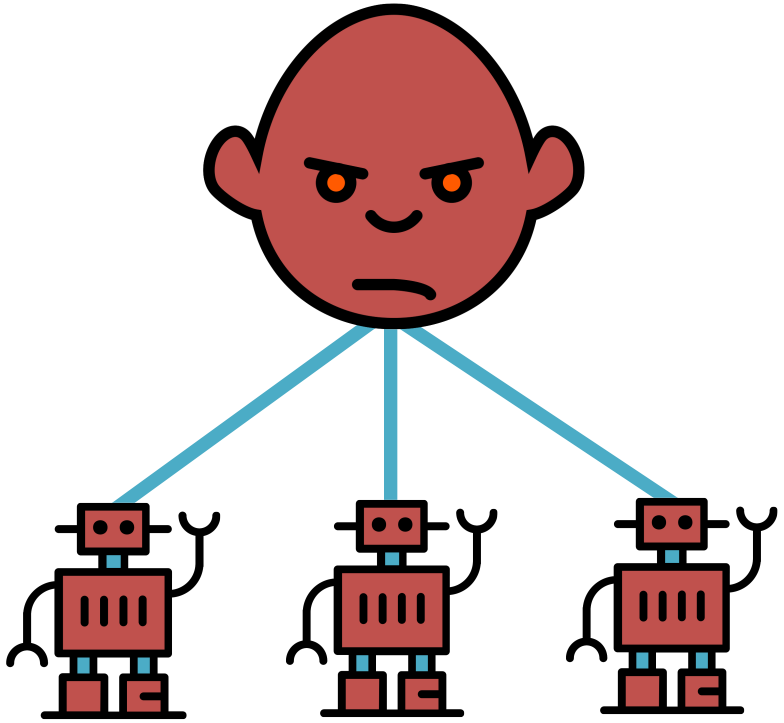
Actors in the Underground

Exploit developers

- Very smart people who reverse-engineer software
- $ Develop and sell exploits packs and kits

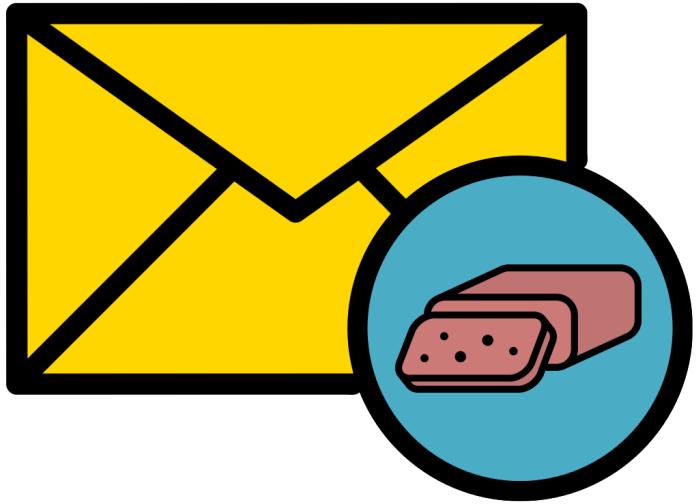
Actors in the Underground



Botnet masters

- Develop software and control vast numbers of zombie machines
- $ Rent out their botnet to other actors

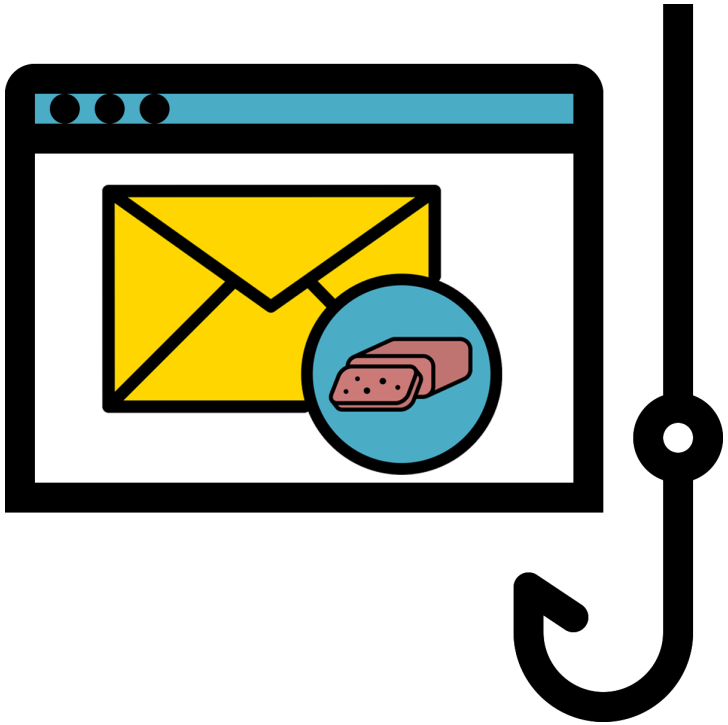
Actors in the Underground



Spammers

- Advertise links for other actors

Actors in the Underground



Phishers

- Setup scam sites to steal information
- Work with spammers to spread the attack

Actors in the Underground

Counterfeiters

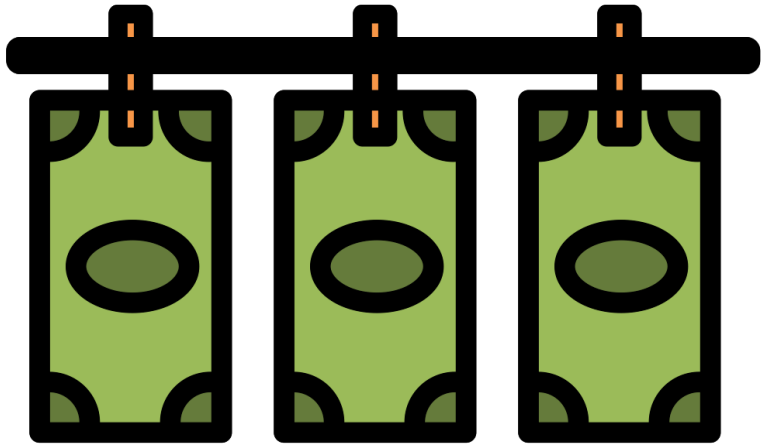
- $ Run websites selling fake goods
- Must be able to clear credit cards

Actors in the Underground

"Bulletproof" Hosting Providers

- $ Offer dedicated servers to other actors
- Hosted in lawless parts of the Internet

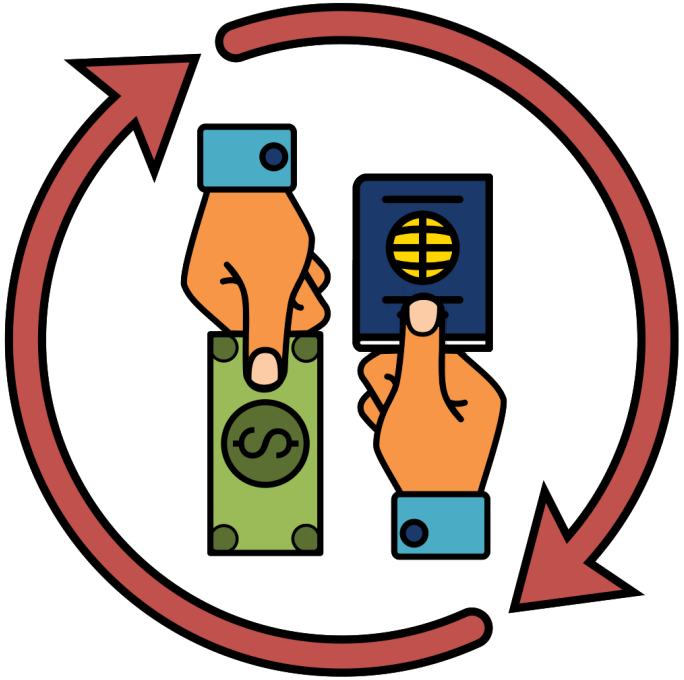
Actors in the Underground



Carders, Cashiers, and Mules

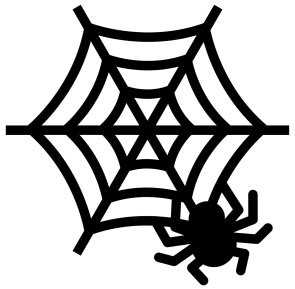
- $ Turn stolen bank accounts and credit cards into cash
- $ Help launder money

Actors in the Underground

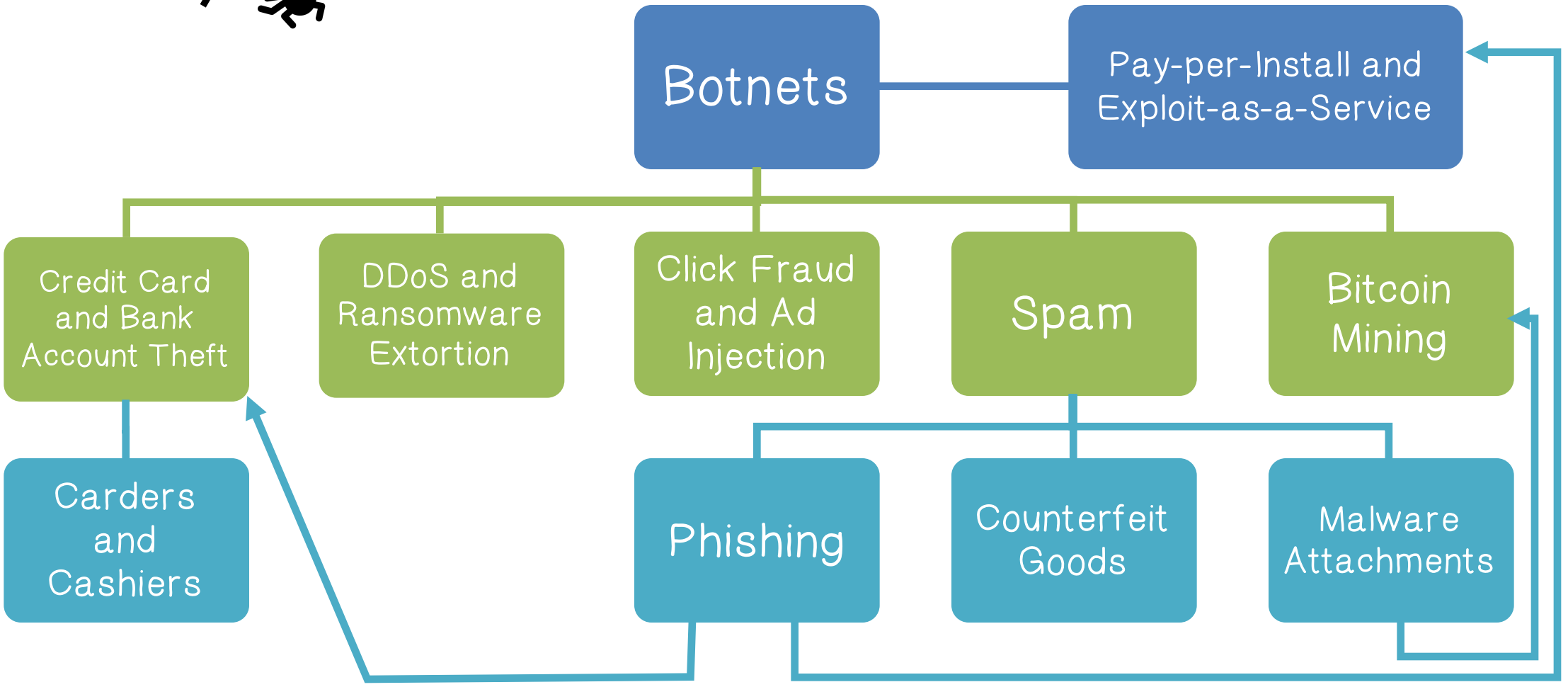


Crowdturfers

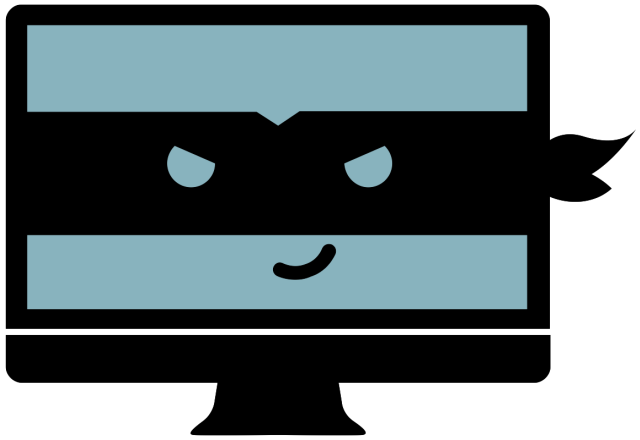
- $ Create, verify, and manage fake accounts
- $ Solve CAPTCHAS for a fee



Structure of the Underground



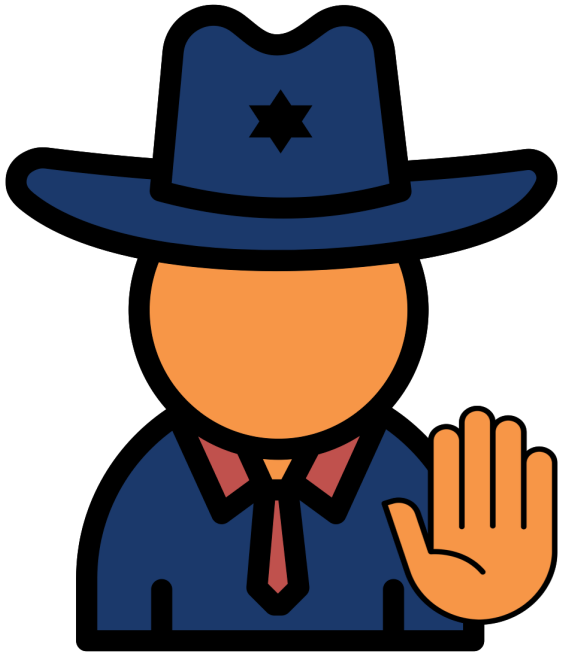
Underground Forums



Today, underground forums are ubiquitous

- Many operate in plain site; they're just a Google search away
- Large volume of illicit goods and services are available

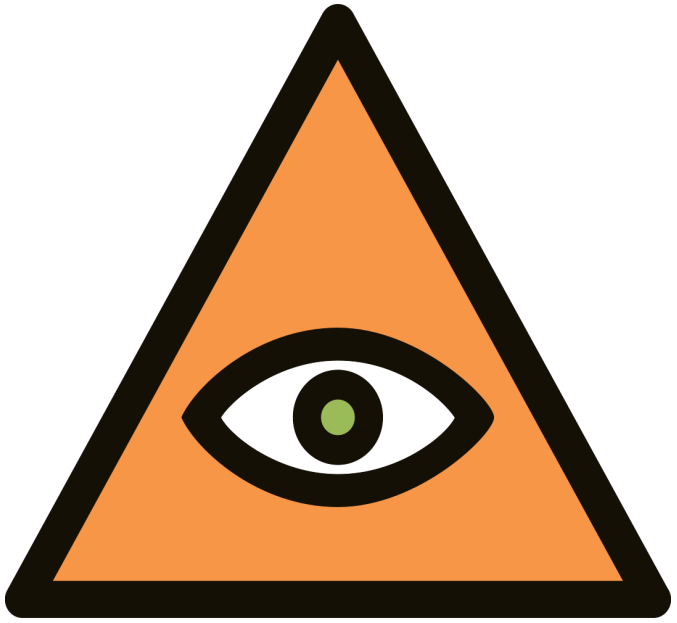
Underground Forums



Law enforcement often targets forums/IRC rooms

- In some cases, forums have been law enforcement sting operations

Underground Forums



Black market forums are hugely valuable for security professionals

- Give researchers a view into the underworld
- Allow white-hats to observe trends and detect unfolding attacks

Underground Forums

Populated by buyers, sellers, and rippers

- Administrators verify trustworthy buyers
- Rippers steal from naïve buyers or sell fraudulent goods

Underground Forums

I have BOA, Wells, and Barclays bank logins...

I have hacked hosts, mail lists, PHP mailer send to all inbox

I need one MasterCard I give one Linux hacked root

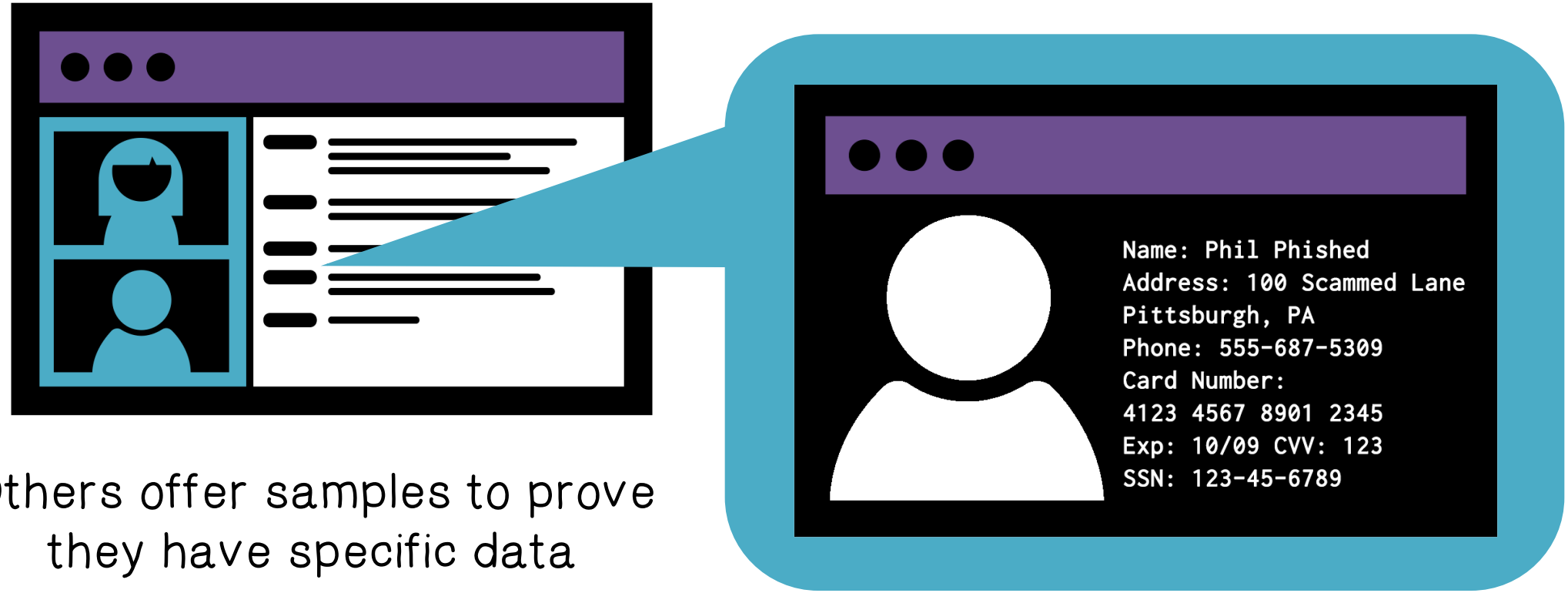
Some participants ask for good or services

Underground Forums

I have verified PayPal accounts with good balance...and I can cash out PayPals

Some participants ask for good or services

Underground Forums



Others offer samples to prove they have specific data

Exploits-as-a-Service: Decoupling and Specialization

In the old days, compromise and monetization were coupled

- Criminals would develop exploits, use them to launch attacks, and then use the hacked machines to make money

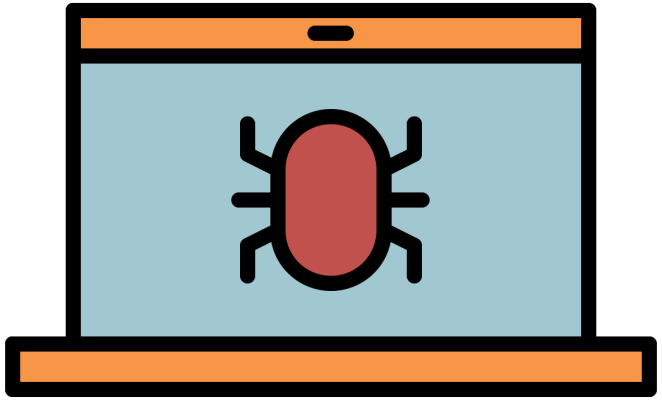
Exploits-as-a-Service: Decoupling and Specialization

Monetization and Compromise are Decoupled:

- Exploit developers sell exploits kits or packers
- Other actors leverage the kits to attack hosts
- Often via spam and/or compromised web servers
- Compromised hosts are then sold on the black market

Pay-per-install model of malware

Exploits-as-a-Service



A malware distribution modelers

- Relies on drive-by-download attacks against browsers
- Blackhole, MPack, and other exploit kits

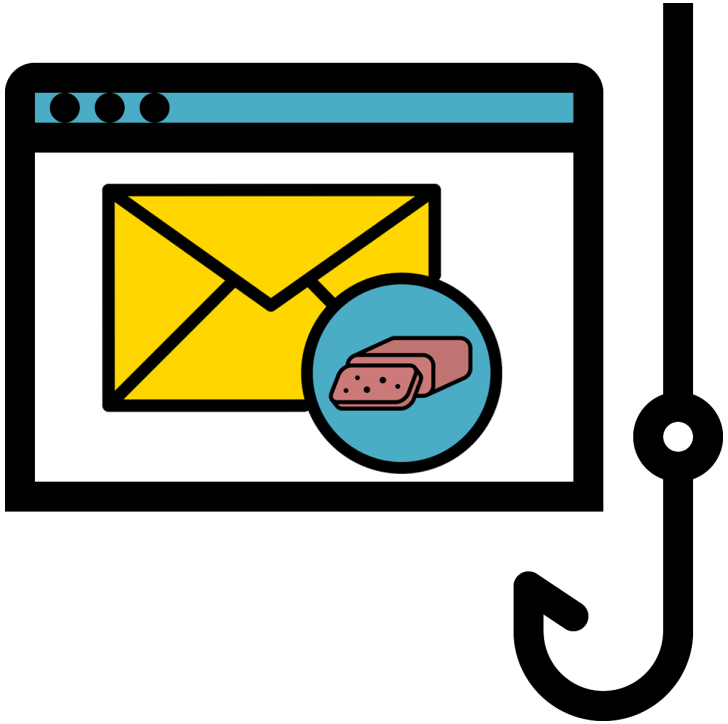
Exploits-as-a-Service

Two styles of attacks:

A miscreant can buy an exploit kit and deploy it themselves

A miscreant can rent access to an exploit server that hosts an exploit kit

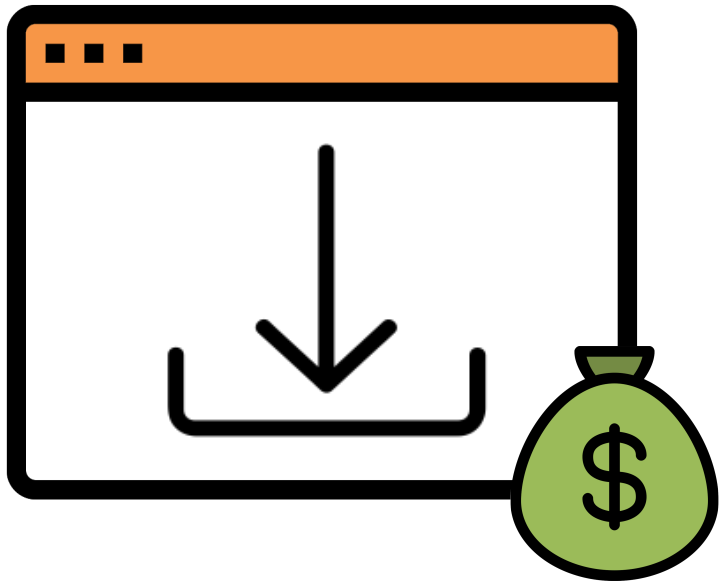
Exploits-as-a-Service



In exploits-as-a-service:

- Miscreants are responsible for acquiring traffic
- And directing victims to the exploit kits using spam or phishing

Exploits-as-a-Service



Traffic-PPI (Pay-per-install) services simplify this process

- Bundle a traffic acquisition mechanism and an exploit server

Dark Web Quiz

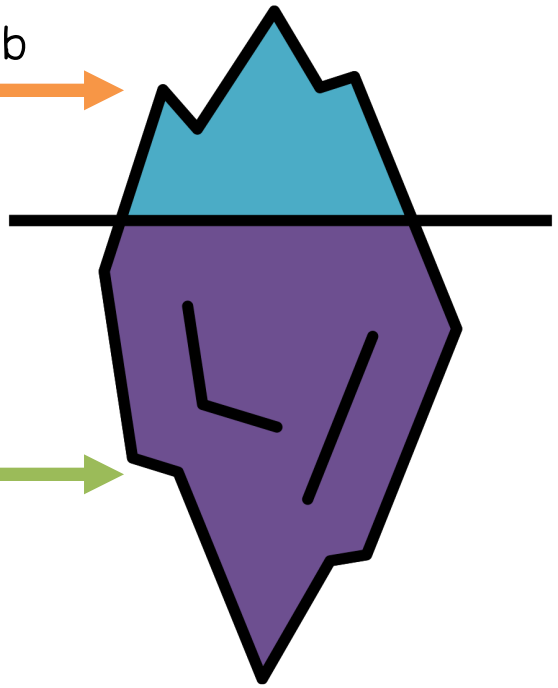
Match the term with its definition:

Attacks:	Descriptions:
B Deep web	A. Readily available to the public, and searchable with standard search engines
C Dark web	B. It is not indexed by standard search engines
A Surface web	C. Web content that exists on darknets

Dark Web Quiz

4% of WWW Content

Surface Web



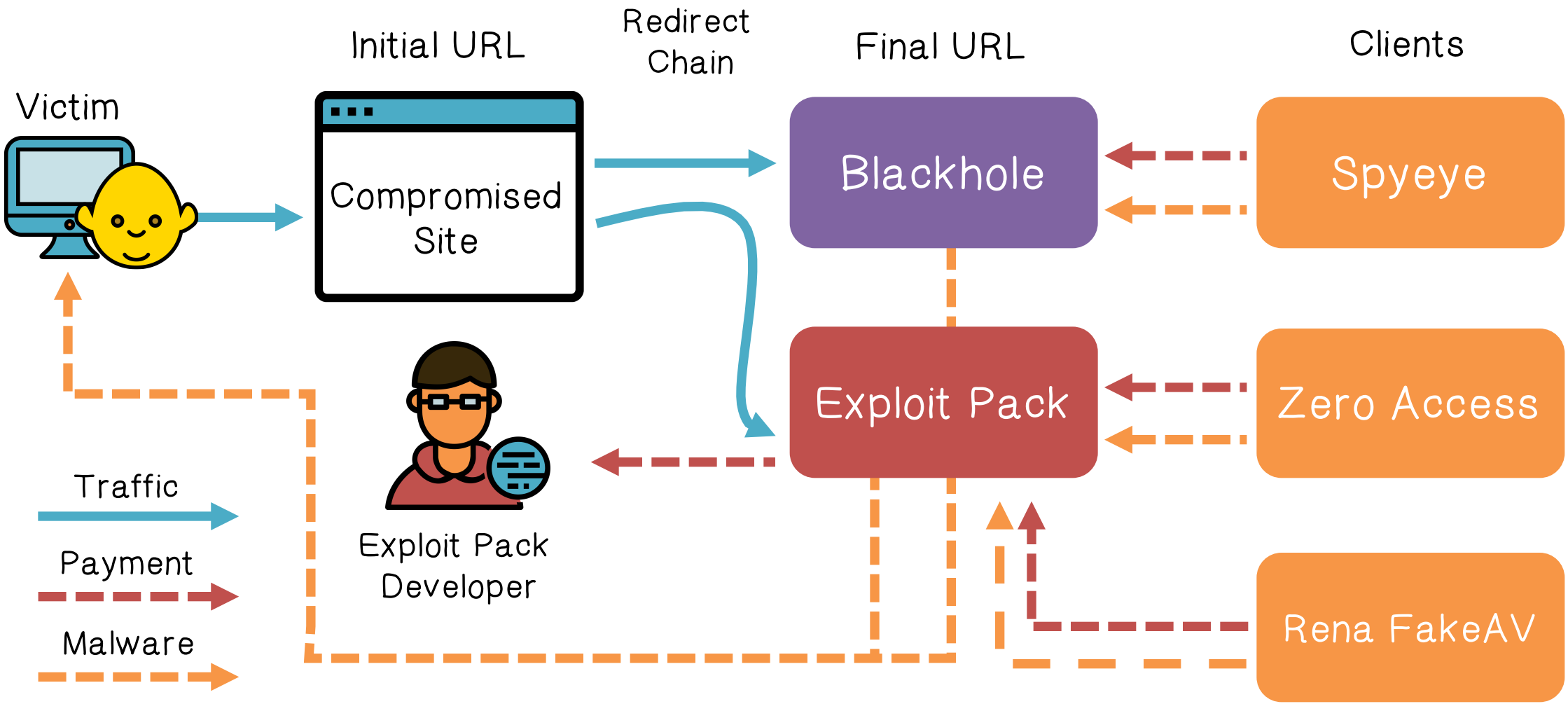
96% of WWW Content

Deep Web

What is the Deep Web?

The Deep Web is the part of the Internet that is hidden from view.

Traffic PPI Example



PPI Quiz

Match the term with its definition:

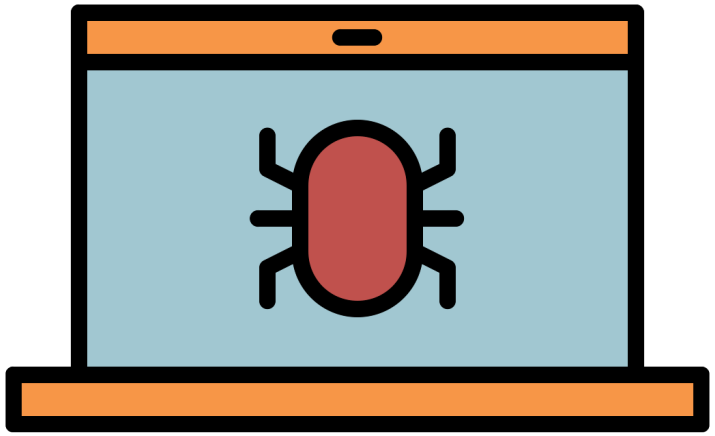
Attacks:

4	Doorway pages
1	Crypters
3	Blackhat Search Engine Optimizer
2	Trojan Download Manager

Descriptions:

1. A program that hides malicious code from anti-virus software
2. Software that allows an attacker to update or install malware on a victim's computer.
3. It increases traffic to the attacker's site by manipulating search engines.
4. A webpage that lists many keywords, in hopes of increasing search engine ranking. Scripts on the page redirect to the attackers page.

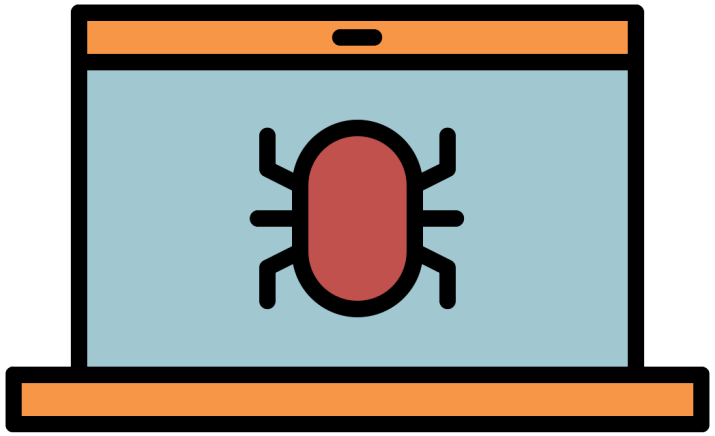
From Malware to Botnets



Infected machines have many other valuable resources

- Unique IP addresses and bandwidth
- Spare CPU cycles

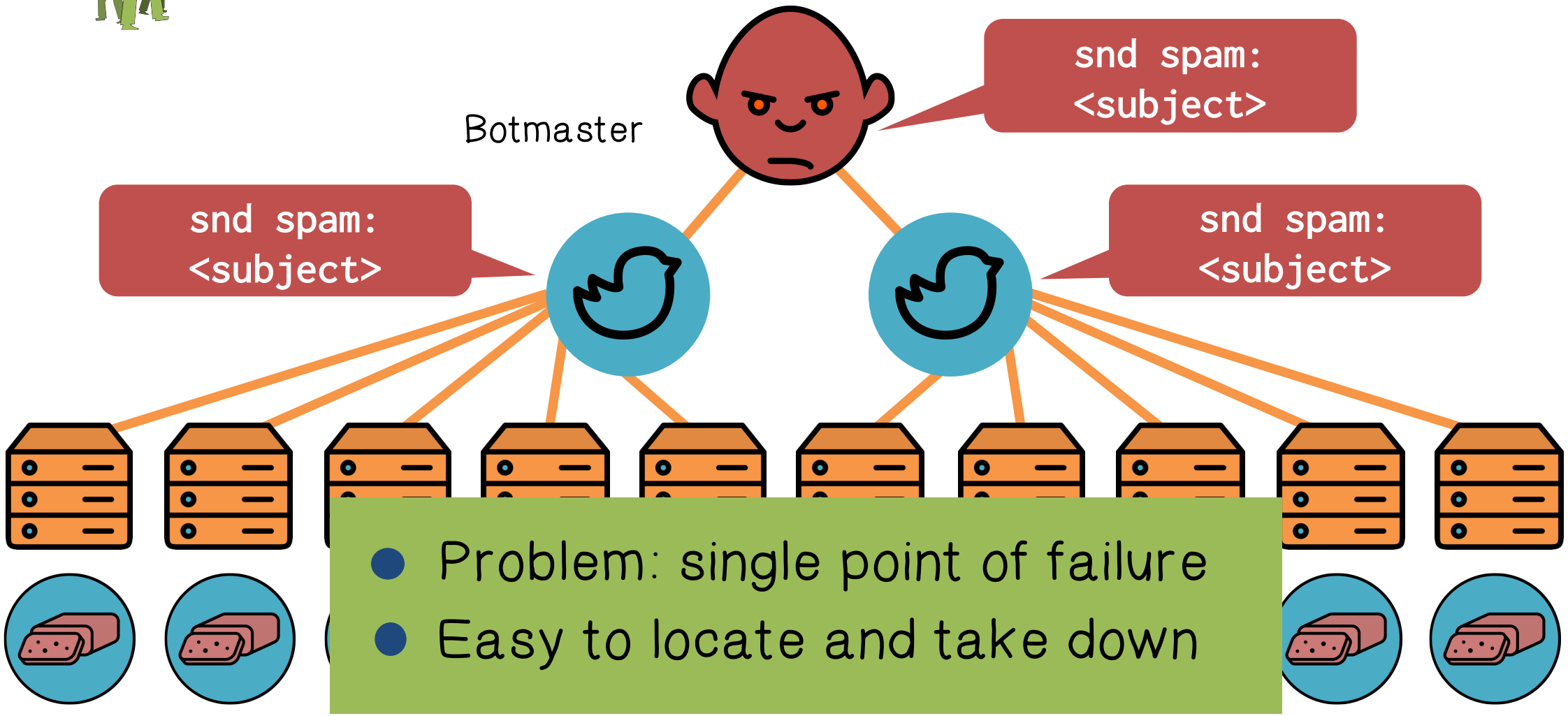
From Malware to Botnets



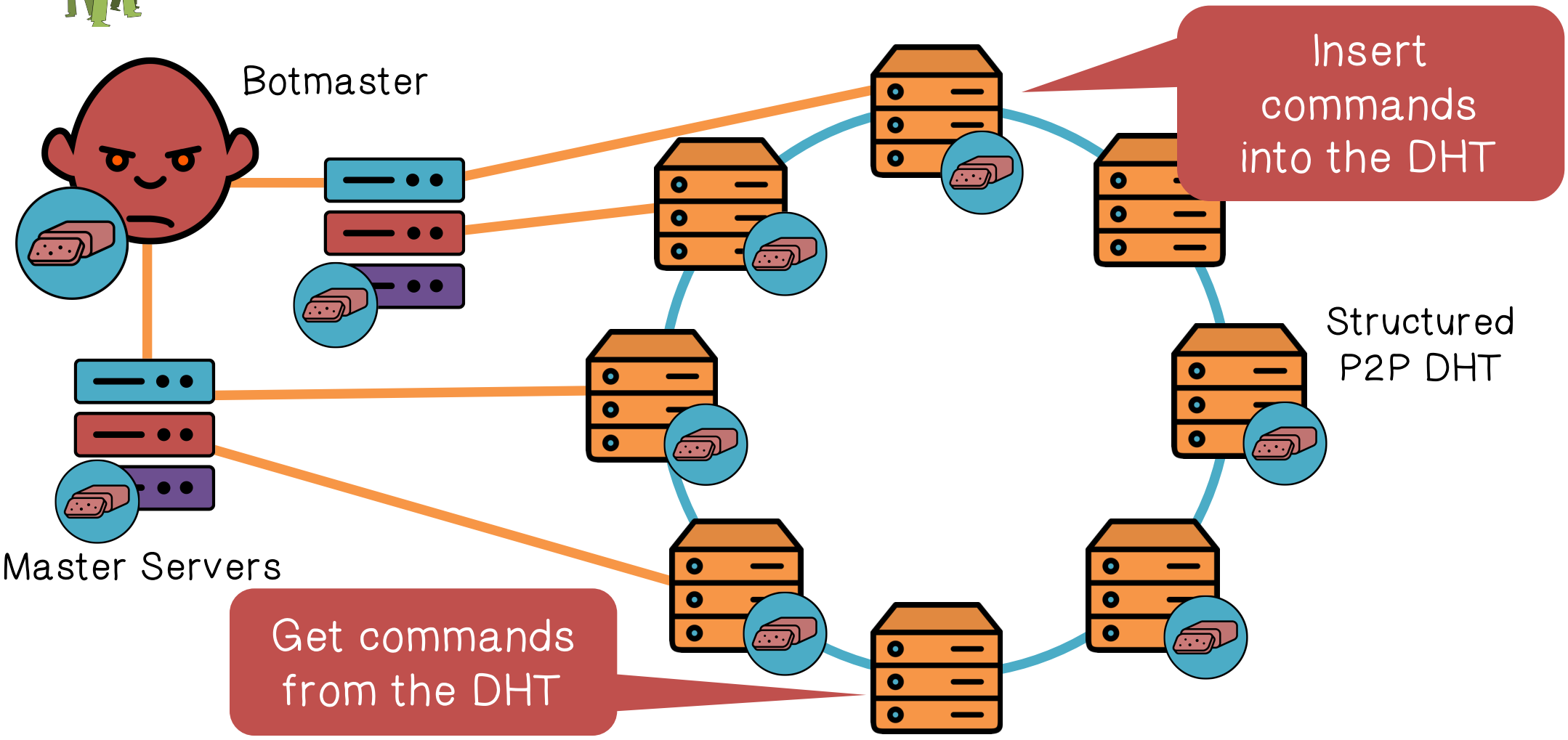
Botnets allow criminals to aggregate and control infected machines

- Command and Control (C&C) infrastructure for controlling bots
- Swaths of bots are often rented out to other actors for various purposes

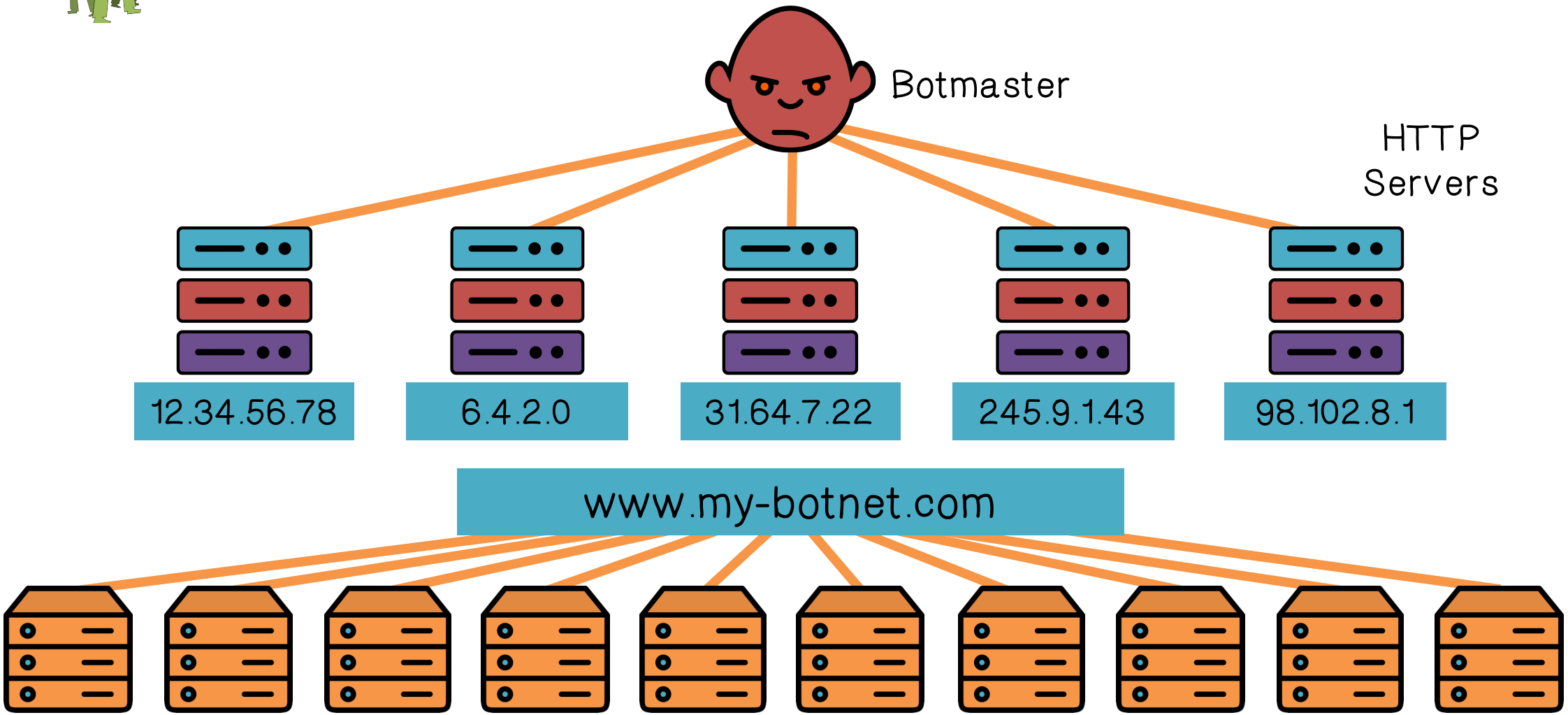
Command and Control : IRC Channels



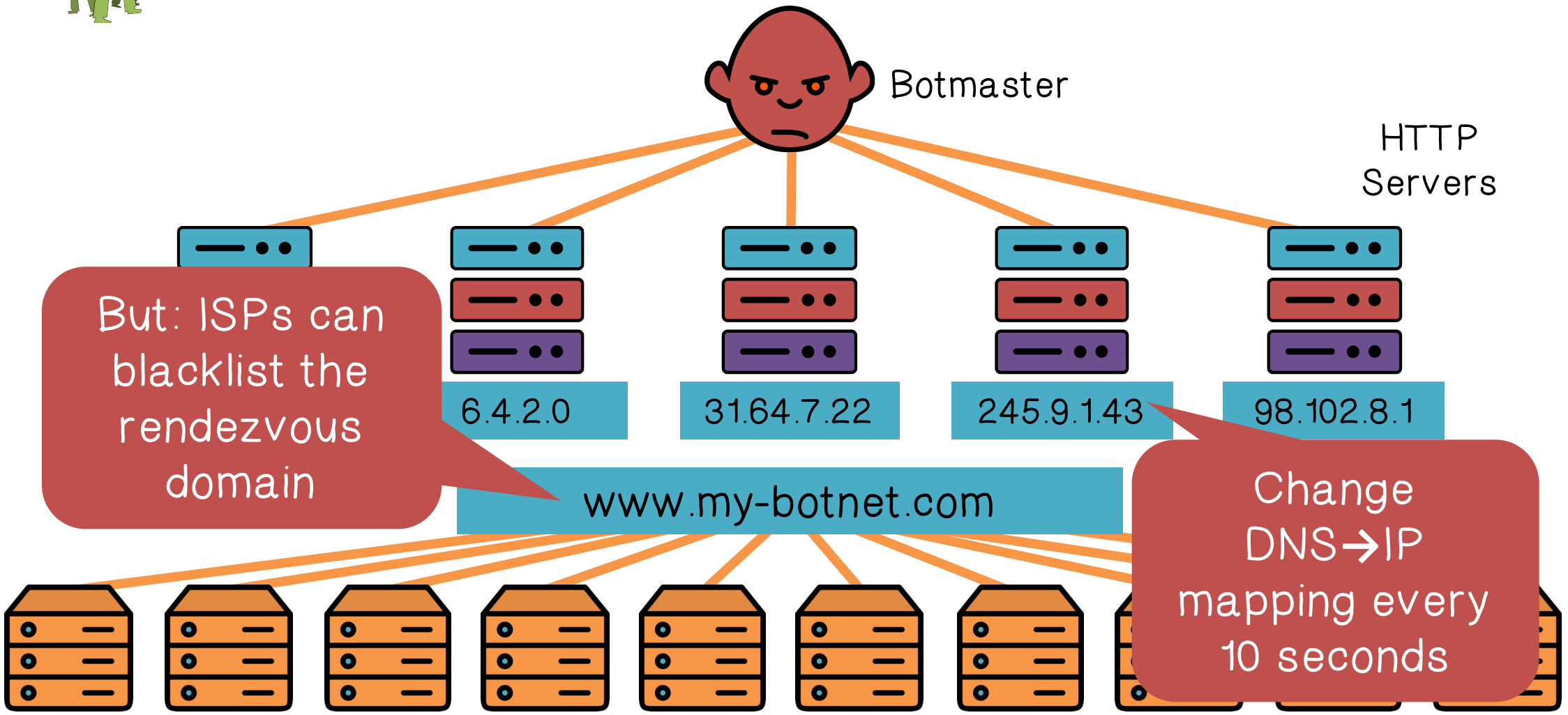
Command and Control : P2P Botnets



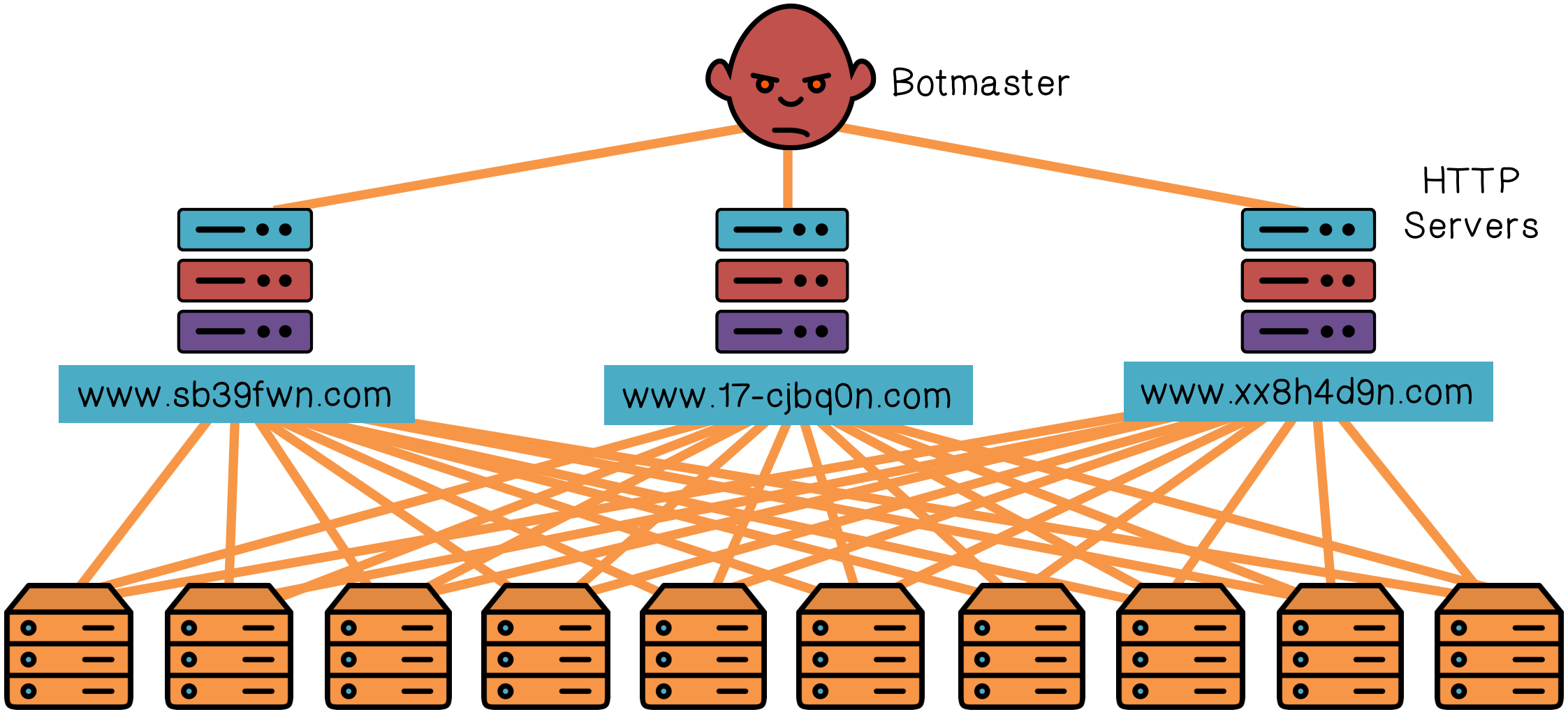
Command and Control : Fast Flux DNS



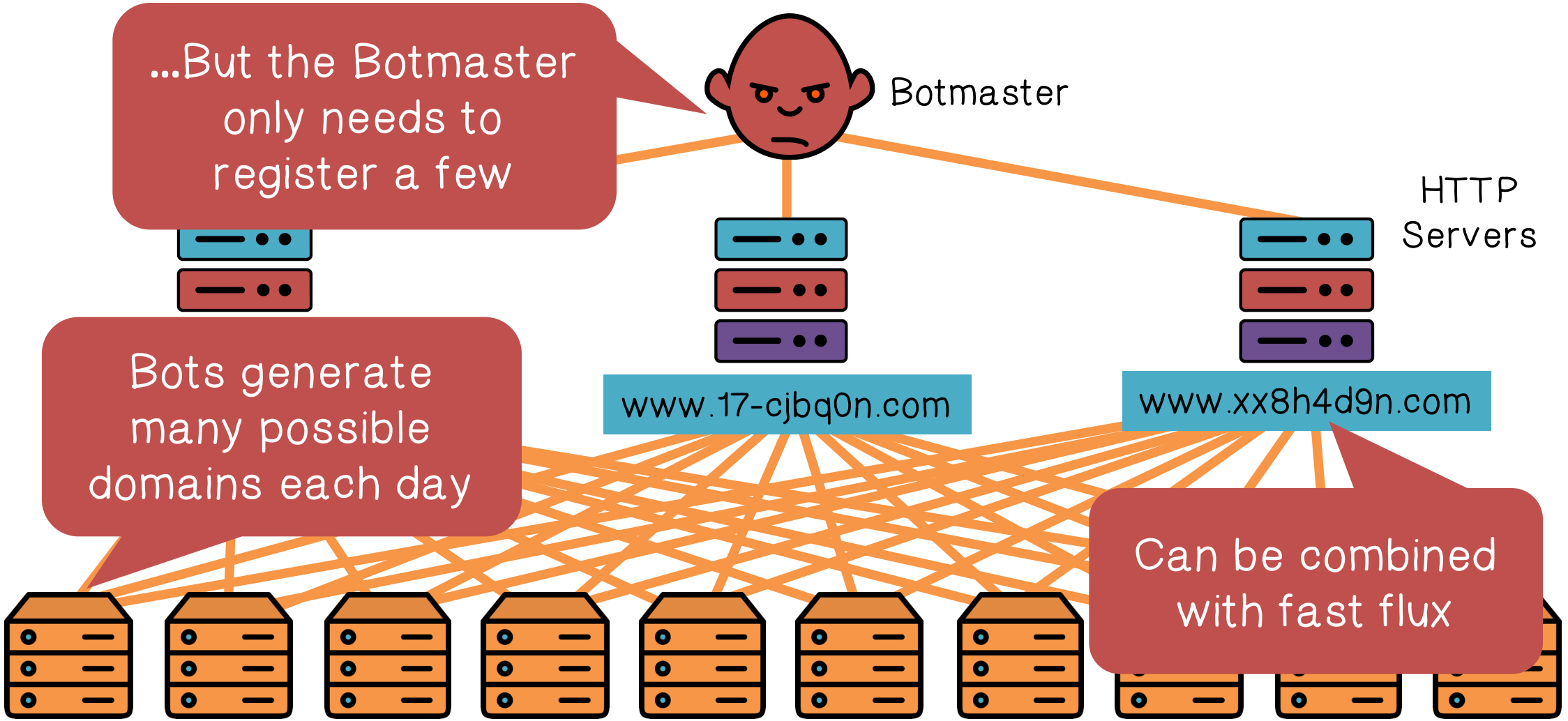
Command and Control : Fast Flux DNS



Command and Control : Random Domain Generation



Command and Control : Random Domain Generation

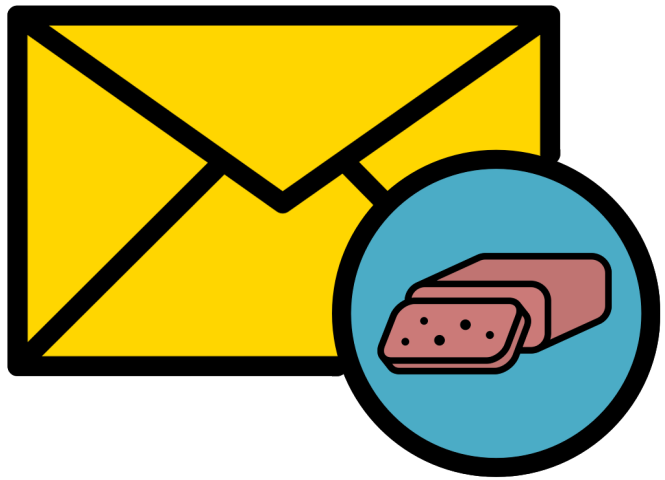


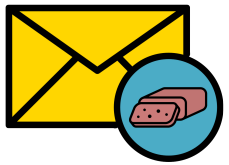
Spam Quiz

What are the two defining characteristics of internet spam?

Inappropriate or irrelevant

Large number of recipients





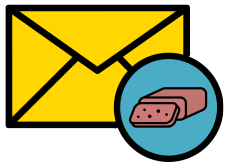
Spam

It is estimated that > 90% of all email sent each day is spam

Hundreds of billions of spam messages per day

Spammers are key players in the cybercrime underground

- Build, curate, buy, and sell lists of email addresses
- Send mail on behalf of other actors for a fee
- Traffic-PPI services looking to acquire traffic and infections
- Phishers looking to steal personal information



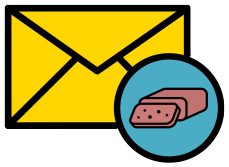
Spam

It is estimated that > 90% of all email sent each day is spam

Hundreds of billions of spam messages per day

Spammers rent access to botnets to send bulk email

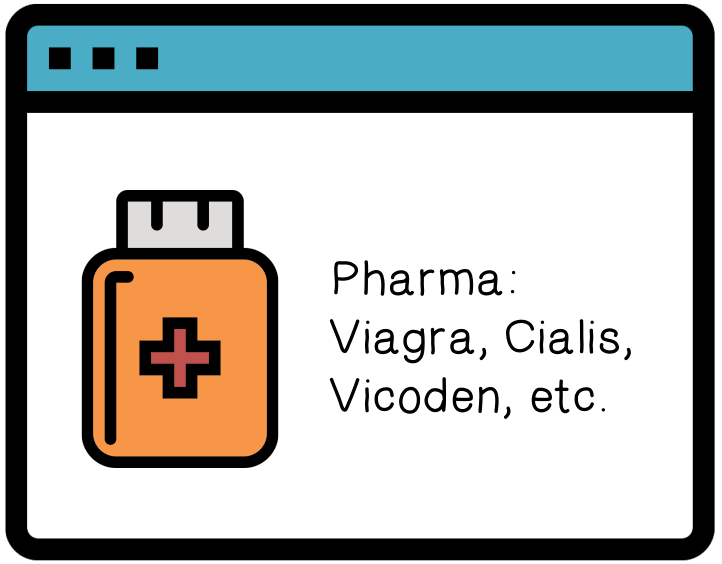
- Need a large number of IP addresses to circumvent spam filters

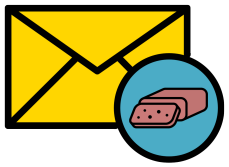


Spam Affiliate Marketing

Huge amounts of spam are related to affiliate marketing schemes

- Scammers set up websites selling counterfeit goods

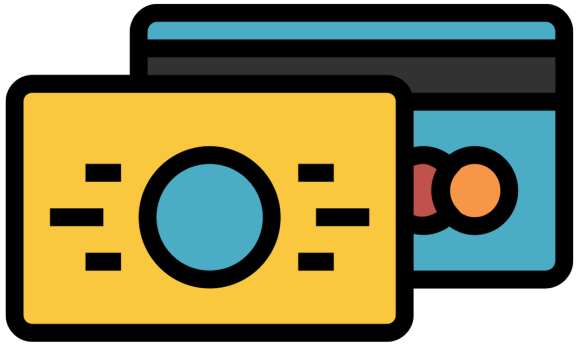


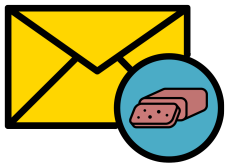


Spam Affiliate Marketing

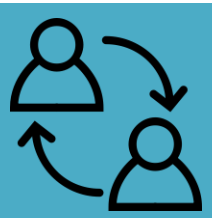
Scammers are responsible for delivering products and collecting payments

- Access to credit card processing infrastructure is crucial
- Many scams have legitimate customer service departments!



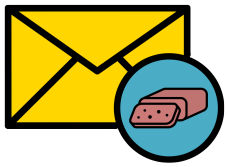


Spam Affiliate Marketing



Spammers sign-up as “affiliates” with scam campaigns

- Spammers advertise the scams, and collect commission on successful sales
- Commission is typically 30-50% of the final sale price



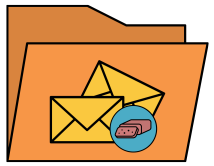
Spam Conversion

Big questions:

- Why do spammers continue to send spam?
- How many messages get past spam filters?
- How much money does each successful “txn” (transaction) make?

Measurement technique:

Infiltrate the spam generation/monetizing process and find out answers



Spam Filter Effectiveness

A case study (Storm botnet):

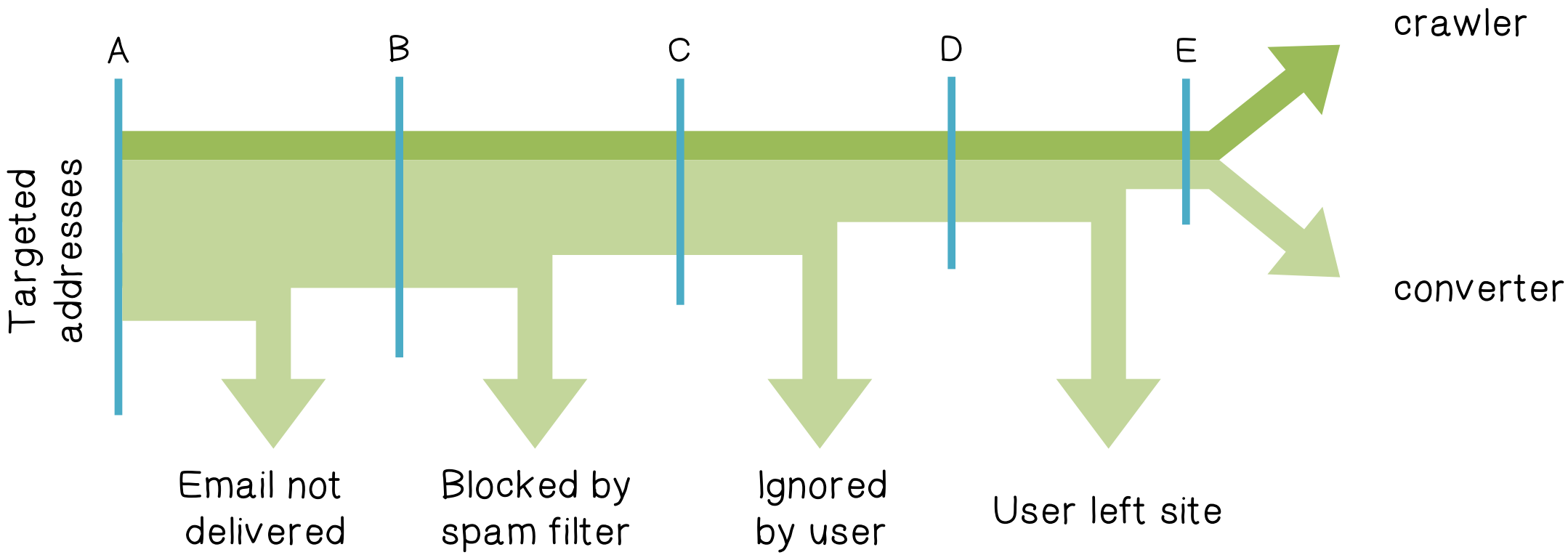
- What percentage of spam got through the filters?

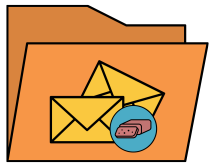
SPAM FILTER	PHARMACY	POSTCARD	APRIL FOOL
Gmail	0.00683%	0.00176%	0.00226%
Yahoo	0.00173%	0.000542%	None
Hotmail	None	None	None
Barracuda	0.131%	N/A	0.00826%

- Average: 0.014%
- 1 in 7,142 attempted spams got through

Spam Filter Effectiveness

A case study (Storm):





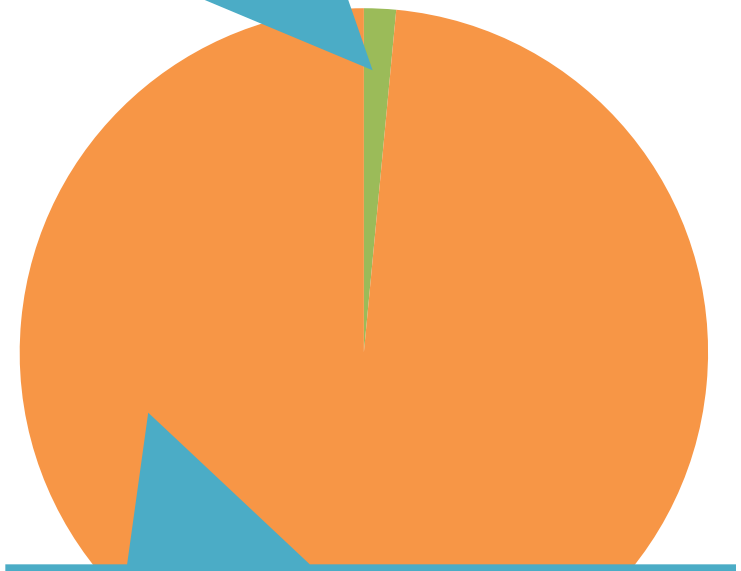
Spam Filter Effectiveness

A case study (Storm):

STAGE	PHARMACY	POSTCARD	APRIL FOOL
A – Spam Targets	347,590,389 100%	83,655,479 100%	40,135,487 100%
B – MTA Delivery (est.)	82,700,00 23.8%	21,100,000 25.2%	10,100,000 25.2%
C – Inbox Delivery	48,662 0.014%	11,711 0.014%	5,618 0.014%
D – User Site Visits	10,522 0.00303%	3,827 0.00457%	2,721 0.00680%
E- User Conversions	28 0.0000081%	316 0.000378%	225 0.000561%
	1 in 1,737	1 in 37	1 in 25

Storm: Pharmaceutical Revenue

1.5% of the sales were tracked $140/day (seems small)



The total for all sales $3.5 million/year (Maybe not so small after all!

28 purchases in 26 days, average price ~$100

But: study only controlled ~1.5% of workers!

Total: $2,731.88, $140/day

$9500/day (and 8500 new bot infections per day) $3.5 million a year

However, this is split with the affiliate program 40% cut for Storm operators via Glavmed ➡ $1.7 million a year

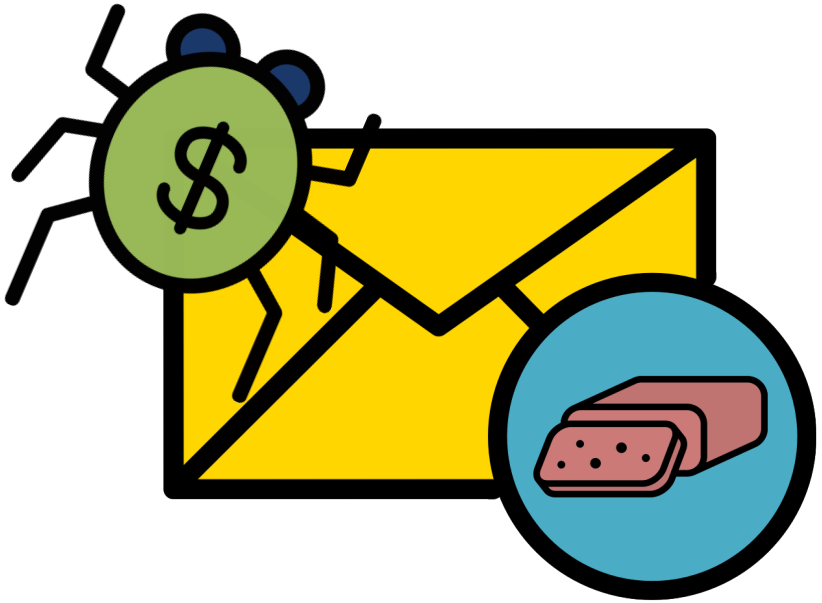
Spam Revenue Quiz

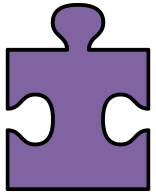
Name the top three countries where spam directed visitors added items to their shopping cart:

United States

Canada

Philippines





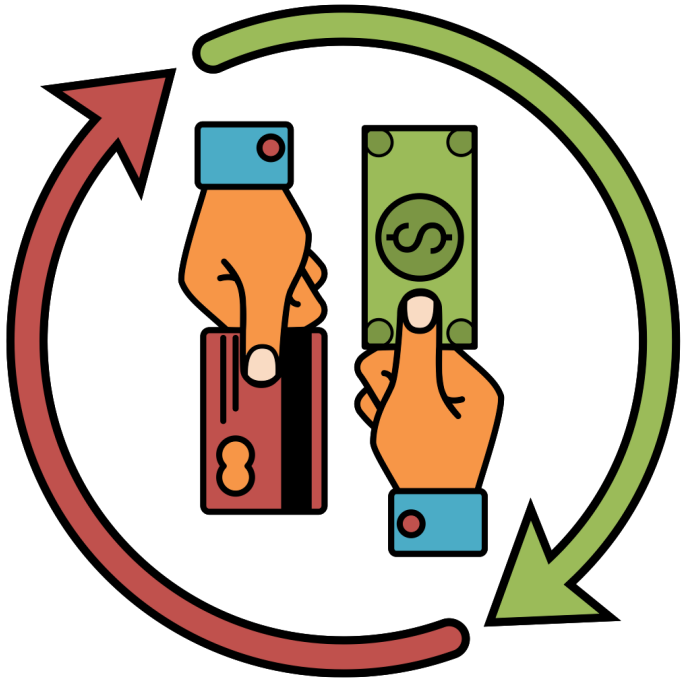
Spam Revenue Quiz

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.

Show Me the Money: Characterizing Spam-advertised Revenue

Scamming Ain't Easy



The scamming ecosystem

- Infrastructure and the key role of payment processors

Example: pharmaceutical scams

Scamming Ain't Easy

Suppose you want to setup
www.canadianpharma.com

What sort of hosting
infrastructure do you need?

Scamming Ain't Easy

Infrastructure	Problem	Solution
Domain name(s)	Legit registrars will take down your name if they receive complaints	Some registrars are known to ignore complaints, but they charge more ;)

Scamming Ain't Easy

Infrastructure	Problem	Solution
DNS servers	DNS servers are an obvious choke-point for law enforcement	"Bulletproof" DNS is available on the market, but its expensive

Scamming Ain't Easy

Infrastructure	Problem	Solution
Web servers	Web servers are an obvious choke-point for law enforcement	"Bulletproof" servers are available, but they're expensive

Scamming Ain't Easy

Some services offer resilient hosting with distributed web servers, domain randomization, and DNS fast-flux.

But obviously, it's expensive!

Scamming Ain't Easy

www.canadianpharma.com

To sell products, you need to be able to accept payments

You'll need:

- Merchant bank account to deposit your payments
- Relationship with a payment processing service
  - Handles credit card payments
  - Withdraws money from the buyers account via a card association network (e.g. Visa)

Scamming Ain't Easy

www.canadianpharma.com

Downfall: Most banks and processors won't do business with scammers

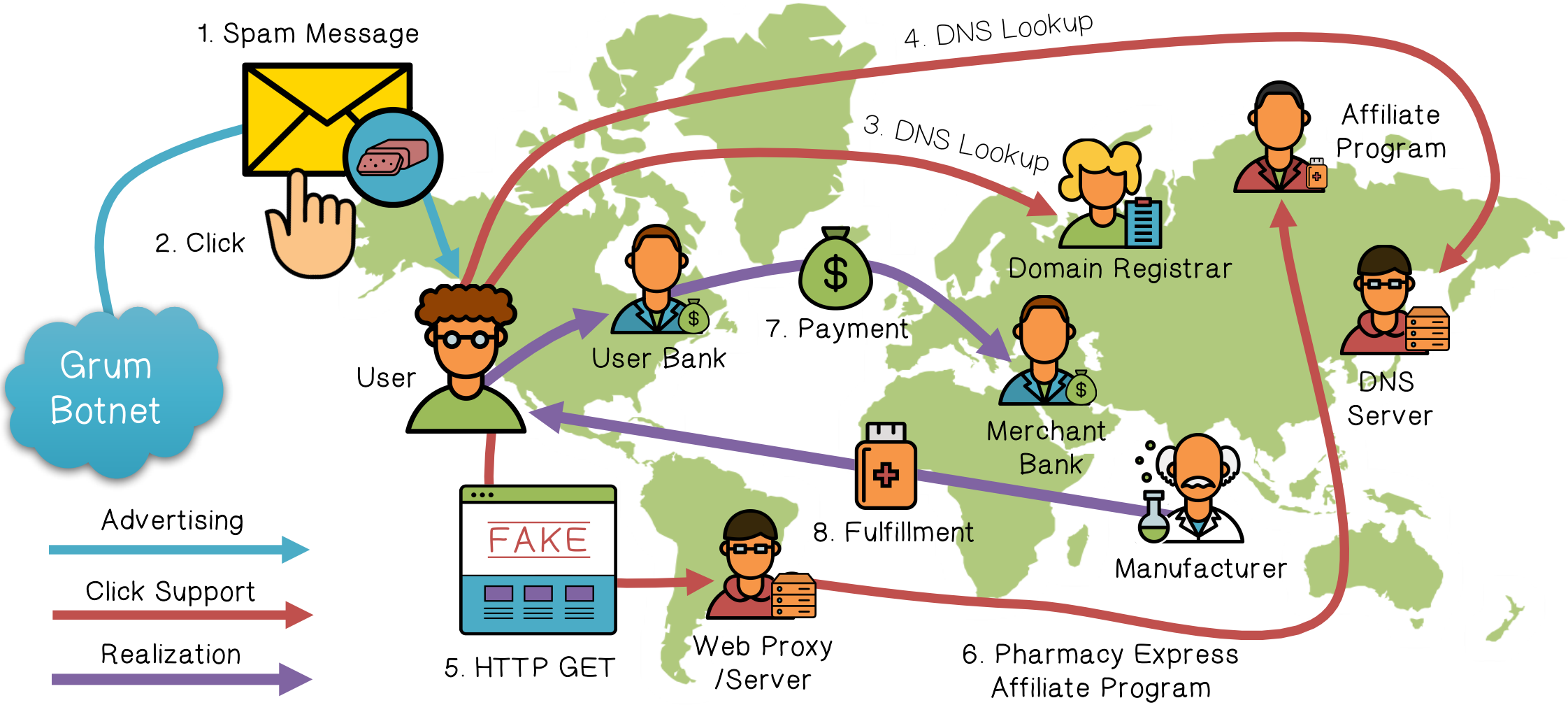
Scamming Ain't Easy

Scam sites almost always ship products to customers

Why?

Unhappy customers → Processor shuts down account → Bank account seized

Example: Pharmacy Express



Example: Pharmacy Express

Affiliate Program		*Distinct Domains*	*Received URLs*	*Feed Volume*
RxPrm	RX–Promotion	10,585	160,521,810	24.92%
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%
GlvMd	GlavMed	2,933	28,313,136	10.32%
Eva	EvaPharmacy	11,281	12,795,646	8.7%
WldPh	World Pharmacy	691	10,412,850	3.55%
PHOL	PH Online	101	2,971,368	0.96%
Aptke	Swiss Apotheke	117	1,586,456	0.55%
HrbGr	HerbalGrowth	17	265,131	0.09%
RxPnr	RX Partners	449	229,257	0.21%
Stmul	Stimul-cash	50	157,537	0.07%
Maxx	MAXX Extend	23	104,201	0.04%
DrgRev	DrugRevenue	122	51,637	0.04%
UltPh	Ultimate Pharmacy	12	44,126	0.02%
Green	Greenline	1,766	25,021	0.36%
Vrlty	Virility	9	23,528	0.01%
RxRev	RX Rev Share	299	9,696	0.04%
Medi	MediTrust	24	6,156	0.01%
ClFr	Club-first	1,270	3,310	0.07%
CanPh	Canadian Pharmacy	133	1,392	0.03%
RxCsh	RXCash	22	287	<0.01%
Staln	Stallion	2	80	<0.01%
	Total	54,220	346,993,046	93.18%

RX-Promotion and GlavMed account for around 35% of all affiliate scams…remember them, we'll see them again :)

				0.79%
				0.48%
				0.61%
				0.24%
				<0.01%
				2.12%
				4.56%
				3.55%
				0.37%
Exqst	Exquisite Replicas	128	620,642	0.22%
DmdRp	Diamond Replicas	1,307	506,486	0.27%
Prge	Prestige Replicas	101	382,964	0.1%
OneRp	One Replica	77	20,313	0.02%
Luxry	Luxury Replica	25	8,279	0.01%
AffAc	Aff. Accessories	187	3,669	0.02%
SwsRp	Swiss Rep. & Co.	15	76	<0.01%
WchSh	WatchShop	546	2,086,891	0.17%
	Total	7,530	15,330,404	4.73%
	Grand Total	69,002	365,395,278	100%

Data collected from spam feeds, botnet infiltration, and various types of honeypots in Fall 2010

Pharmaleaks

In 2012, the databases for GlavMed, SpamIt, and RX-Promotion were breached, dumped, and publicly released

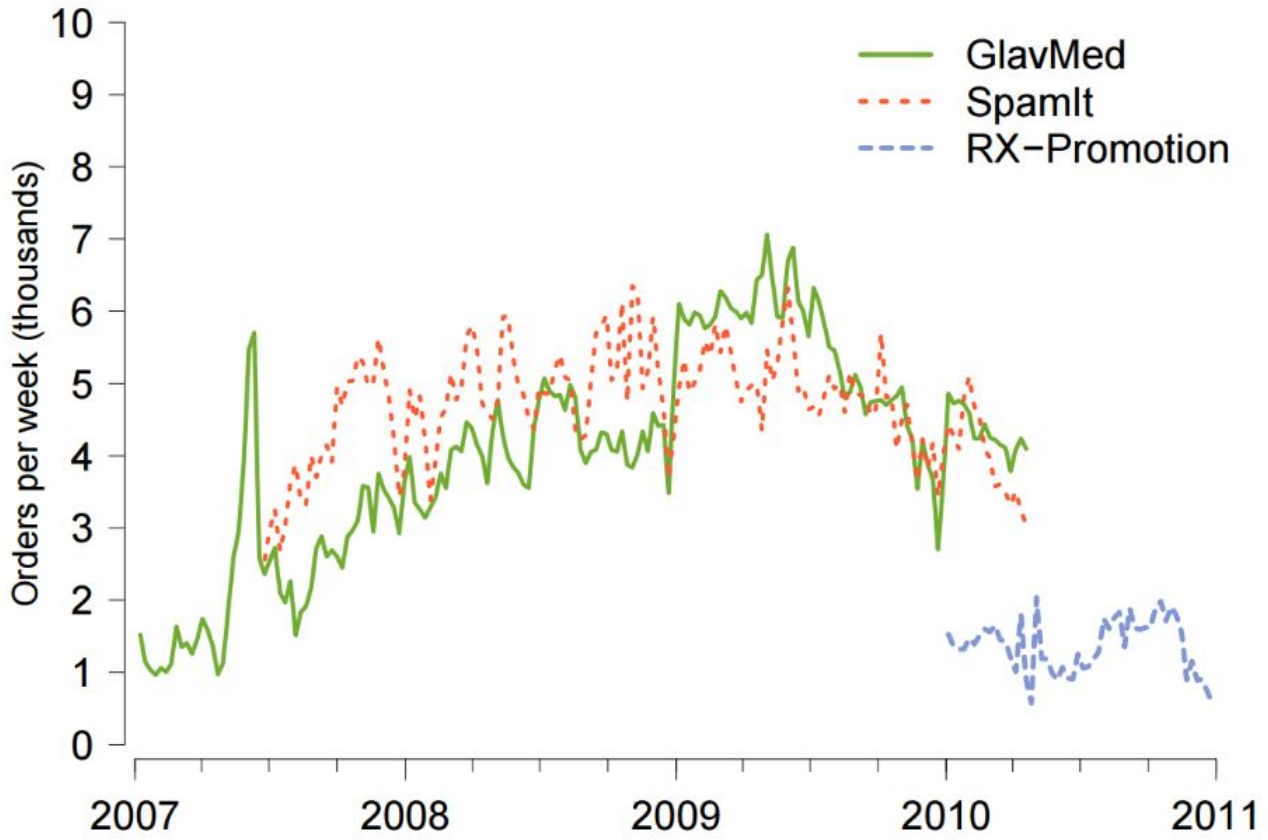
The databases contained complete logs of sales, customers, and affiliate relationships

Program	Period	Affiliates	Customers	Billed orders	Revenue
GlavMed	Jan 2007 – Apr 2010	1,759	584,199	699,516	$81M
SpamIt	Jun 2007 – Apr 2010	484	535,365	704,169	$92M
RX-Promotion	Oct 2009 – Dec 2010	415	59,769 – 69,446	71,294	$12M

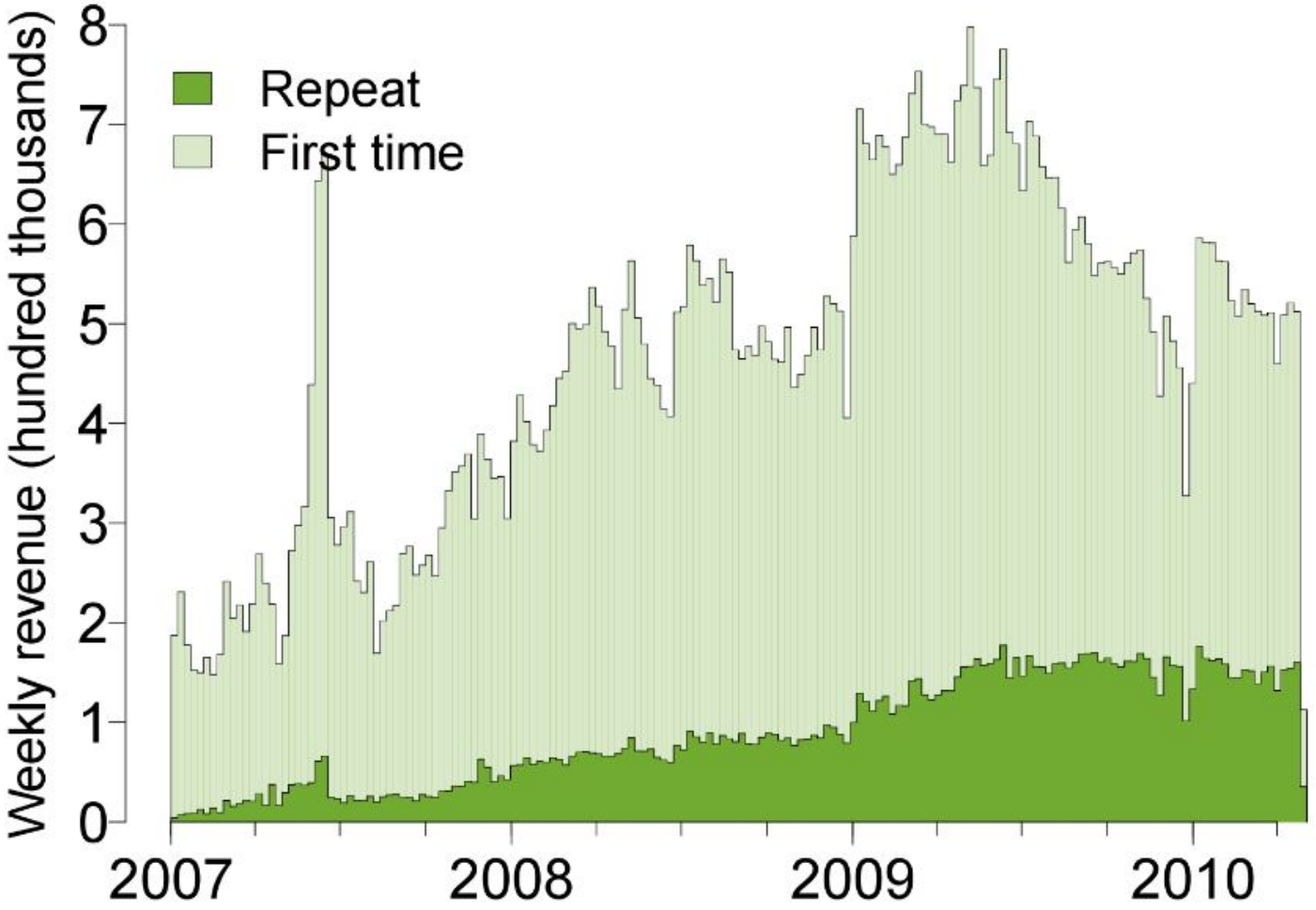
Source: *PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs*

Pharmaleaks

Transaction Volume



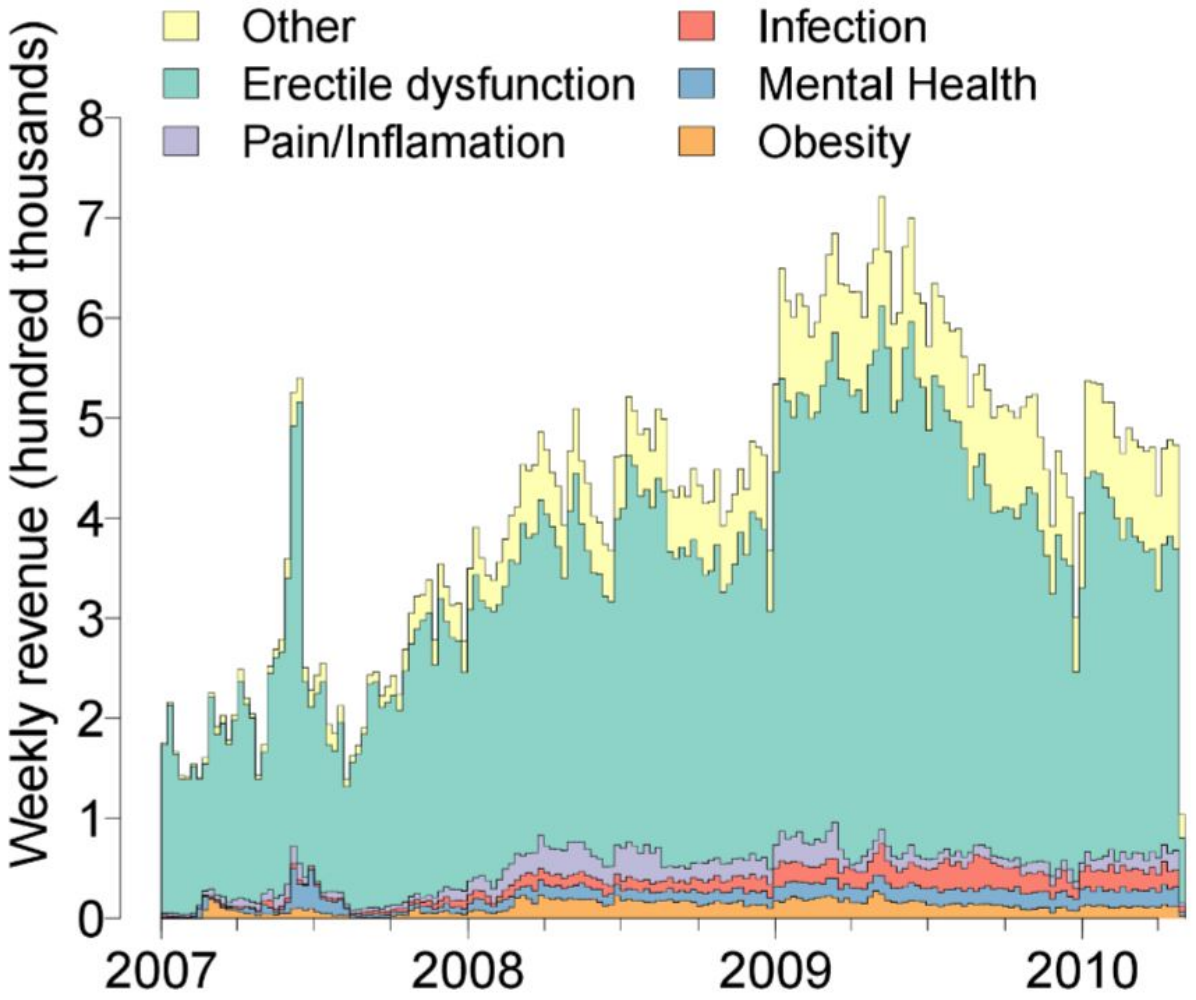
Pharmaleaks



New vs. Repeat Customers

Pharmaleaks

Types of Products



Profit

Payments to affiliates

Bulletproof hosting

Spammers and botnet operators

	RX-Promotion March – September 2010	
Gross revenue	$7.8M	
Direct costs	$5.5M	(70.8%)
Commissions	$3M	(38.1%)
Suppliers[a]	$1.4M	(17.6%)
Processing	$1M	(13.2%)
Other direct	$148.3K	(1.9%)
Indirect costs	$1004K	(12.8%)
Administrative	$197K	(2.5%)
Customer service	$124K	(1.6%)
Fines	$107K	(1.4%)
IT expenses	$202K	(2.6%)
Domains	$114K	(1.5%)
Servers, hosting	$66K	(0.8%)
Selling expenses	$315K	(4%)
Marketing	$105K	(1.3%)
Lobbying	$157K	(2%)
Other indirect	$134K	(1.7%)
Net revenue	$1.3M	(16.3%)

[a] Costs of goods and shipping are combined.