Economic Incentives and Underground Economies

CMSC 414

December 4, 2017

Economics

Money drives both attack and defense

- What data is for sale?
- By whom?
- How?
- Who is buying?

Attackers buy this, but so do

- AV vendors
- Firewall vendors
- Software developers

Understand incentives ⇒ Find choke points

Why is Everything So Bad?

Externalities

- Everybody says they want security
- Nobody wants to pay extra for security
- Everybody actually wants features
- Security only noticeable when it fails

Secure software

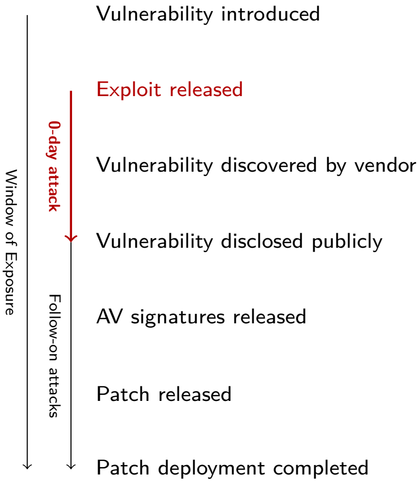
- Costs more to develop and maintain
- Provides no benefit to companies
- Costs companies nothing to neglect

Actual software/system security requires *either*

- Customer demand (make it worthwhile for developers)
- Regulation (make it mandatory for developers)

We have *neither*

Zero-Days



Vulnerability introduced

Exploit released

Vulnerability discovered by vendor

Vulnerability disclosed publicly

AV signatures released

Patch released

Patch deployment completed

Window of Exposure

0-day attack

Follow-on attacks

Discovered by

- Security researchers
- Random hackers
- Organizations (criminal or nation-state)

Bought by

- Software vendors
- Malware authors
- Organizations (criminal or nation-state)

Payment via

- Bug bounties
- Exploit brokers

Buying and Selling Zero-Days

Big business!

Exploit brokers act as *middlemen*
⇒ Match buyers/sellers for a commission

Payments often continue until vulnerability disclosed

The bigger the target, the more they sell for

- $5k–$30k for Adobe Reader
- $100k–$250k for iOS

Spam

Costly nuisance

- Delivery/storage costs for email providers
- Filtering requires hardware/time
- Annoys users who receive it
- Leads to malware infections, fraud, ...

How do we fight spam?

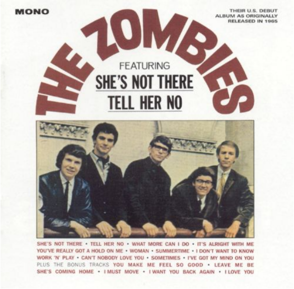
- At delivery ⇒ See costs above
- Try to understand *why* it exists, how it works
  ⇒ *Can we disrupt it?*

Limitations on Spam

One server sends lots of spam
⇒ Block it!

Spoof the source address?
⇒ Email uses TCP, so must complete 3-way handshake

What's a spammer to do?
⇒ Use a botnet!


MONO
THEIR U.S. DEBUT ALBUM AS ORIGINALLY RELEASED IN 1965
THE ZOMBIES
FEATURING
SHE'S NOT THERE
TELL HER NO
SHE'S NOT THERE • TELL HER NO • WHAT MORE CAN I DO • IT'S ALRIGHT WITH ME
YOU'VE REALLY GOT A HOLD ON ME • WOMAN • SUMMERTIME • I DON'T WANT TO KNOW
WORK 'N' PLAY • CAN'T NOBODY LOVE YOU • SOMETIMES • I'VE GOT MY MIND ON YOU
PLUS THE BONUS TRACKS YOU MAKE ME FEEL SO GOOD • LEAVE ME BE
SHE'S COMING HOME • I MUST MOVE • I WANT YOU BACK AGAIN • I LOVE YOU

What Happens When You Click on a Spam Link?

Most spam contains a URL to click on
⇒ Block that URL, or get them TOSed[1]!

Avoid this by

- Use URL shorteners (`bit.ly`, `tinyurl.com`, ...)
- Have lots of URLs (randomly generated hosts/domains)
- Can redirect to a single server, or one of many (ie, replication for censorship avoidance)

Eventually end up at a *storefront*

[1] Report a server to its provider for violating its *Terms of Service*, in an effort to have them shut down

Bulletproof Hosting

Most people don't like spam or spammers

Scams and fraud also generally frowned upon

Hosting, name service, domain registration vulnerable to take-downs

For enough money, **Bulletproof Hosting** services

- Won't block you
- Won't take your servers down

Frequently associated with organized crime

Legitimate uses, too: *dissident groups* and *whistleblowers*

The bad guys use the same technologies as the good guys
$\Rightarrow$ Only way to stop the former also stops the latter

Fast-Flux DNS

DNS records have a Time-to-Live (TTL)

- Measured in seconds
- Expires ⇒ Invalidate cached records

In **Fast-Flux DNS**, this TTL is small (minutes to hours)

Hostname to IP addr binding changes often
⇒ Hard to filter IP addresses

Spammers use *proxies* as spam URLs

- Fast-Flux proxy DNS records
- Proxies redirect to more-stable addresses

Not all uses of Fast-Flux DNS are malicious

Group Exercise 1

The `econ` repository's README file has your exercises for today. Task 1 deals with Fast-Flux DNS bindings, both good and bad.

DO NOT VISIT ANY OF THE SERVERS YOU FIND WHEN LOOKING THROUGH SPAM-ORIGINATING HOSTNAMES!

Botnets as Business

Botnets are big business

Can be used to:

- Steal data via keylogging, etc
- Propagate ransomware
- Launch man-on-the-side attacks (piggyback malicious transactions)
- Perform DDoS-for-hire
- Engage in click fraud
- Host rogue services
- Send lots of spam

Impact on users of infected machines almost negligible
⇒ May not even notice or care

Fighting Botnets

How do we fight botnets?

Prevent initial infection ⇒ Hard!

Botnets rely on a **Command-and-Control** (C&C) server
⇒ Often called a *Bot Herder*

Take down the bot herder, the botnet goes idle

- Move the herder around frequently
- Bots configured with list of possible herder nodes
- Try nodes at random, looking for current herder
- Herder responds with signed messages

These guys are pretty good at building robust distributed systems!

Specialization

Building a house requires lots of people with different skills

- Architects
- Excavation crews
- Carpenters
- Electricians
- Plumbers
- Roofers
- etc.

Same thing in scams/black markets
⇒ Not everyone is able/wants to do everything

Focus on what you're good at, and hire out your services!

Affiliate Programs

Affiliate Network provides

- Domain purchasing
- Web storefronts and shopping carts
- Customer analytics
- Advertising templates

Spammers

- Pay bot herders to send spam
- Get a commission from Affiliate Program for completed sales

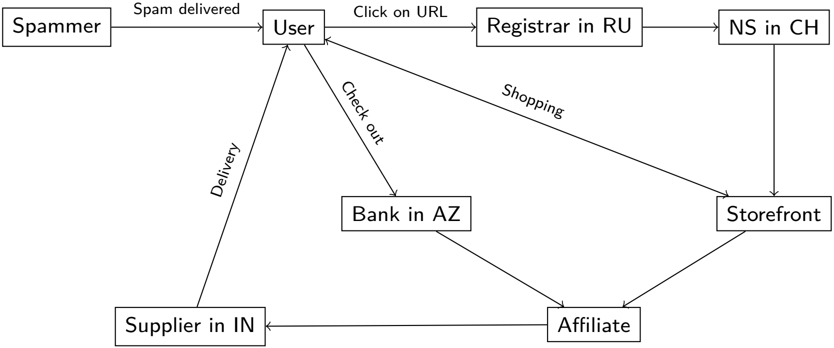
Affiliate Network hands off completed sales for

- Payment processing
- Shipping/fulfillment

Can also be used to buy/sell 0-days, malware vectors, ...

Value Chain

How does all this tie together?



What do People Buy?

Mostly

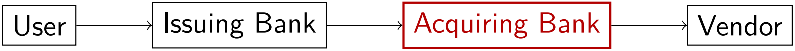
- Pharmaceuticals (apparently legit!)
- Replica luxury goods (cheap junk!)
- Counterfeit software (apparently legit!)

Small number of affiliate programs

Stage	**Pharmacy**	**Software**	**Replicas**	**Total**
URLs	347M	3M	15M	365M
Domains	54k	7k	7k	69k
Web clusters	968	51	20	1039
Programs	30	5	10	45

Acquiring Banks

This is where payments go



User → Issuing Bank → Acquiring Bank → Vendor

This is the weak point!

- Not too many banks willing to work with criminals
- Take one out, even fewer options
- Going after complicit banks discourages other banks from similar behavior

Payment and Fulfillment

Scammers take Visa and Mastercard

- Widely available (at least in the West)
- Convenient (again, at least in the West)

They use the correct product codes

- No real reason not to
- Payment processors not big fans of incorrect codes

Fulfillment rate actually pretty good

- Want repeat customers
- Failure to deliver could lead to charge-backs
  ⇒ Issues with banks
- Fraud charges are more serious

Alternative Payment Methods

I don't want to give these guys my credit card...

Pre-paid credit cards are safer
⇒ More of a pain to get for each purchase

How about BitCoin?

Pros:

- No card number in black marketeers' hands
- Public key not tied to your identity

Cons:

- No ability to protest charges
- More likely to lead to lack of order fulfillment

Group Exercise 2

Task 2 has you explore some more ways of filling in the knowledge gaps for scammer networks.