Cybercrime Markets
Operation

Dr. Luca Allodi
Security Group, WIN, TU/e

Cyber Attacks and Defenses
Q2 2019

Cybercrime – 101 definition

• Cybercrime is an extension of “traditional crime”
  • Happens in forms vehiculated by a technological system
• Technological systems can be:
  • Vehicle to crime \(\rightarrow\) target is outside of the technological-IT domain
  • Vehicle & target of crime \(\rightarrow\) impact is suffered by a (group of) tech. system(s)
    • Can possibly extend to users of those systems

• Tech system
  • Traditional computers
  • Services
  • Mobile
  • Hw tokens ...

• Crime related to
  • Malware/attacks/data
  • Drugs
  • Weapons
  • Human trafficking
  • Terrorism
  • Child exploitation
  • Social disturbance
  • ...

Not for sharing - Dr. Luca Allodi (TU/e) – Underground cybercrime economics
Provision and trade of illegal goods

• Migration of (some) “offline” criminal activities online

<table>
<thead>
<tr>
<th>Provision</th>
<th>Trade</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hacking</strong></td>
<td><strong>Largely online</strong></td>
</tr>
<tr>
<td>• First order (enabling the hack)</td>
<td>• Product selection, “contract”, and delivery</td>
</tr>
<tr>
<td>• Vulnerabilities, exploits, ..</td>
<td></td>
</tr>
<tr>
<td>• Second order (after the hack)</td>
<td></td>
</tr>
<tr>
<td>• Credit cards, banking info, trade secrets, ..</td>
<td></td>
</tr>
<tr>
<td><strong>Non-hacking</strong></td>
<td><strong>Mix of online and offline</strong></td>
</tr>
<tr>
<td>• Drugs, weapons, stolen HW, etc..</td>
<td>• Offline == delivery of physical good</td>
</tr>
<tr>
<td>• Mostly physical “goods”</td>
<td></td>
</tr>
</tbody>
</table>

“Fair” trade (in the underground?!) 

• Markets are made of contracts between agents; examples:
  • I’ll give you X $ for exploit Y;
  • I’ll give you K $ for malware J; etc.

• A market only operates if the contracts are valid/can be satisfied

• Agency theory → how do economic agents stipulate contracts?
  • “Principal” → asks for service; “Agent” → provides service
  • The information that principal and agent have is key to achieve a sustainable
    market equilibrium:
    • Best strategy for the seller → deliver the good as promised
    • Best strategy for the buyer → respect terms as agreed
Information asymmetry & markets

• First defined in the Market for Lemons by Akerlof

• Ingredients for market failure:
  1. The Agent/service provider knows much more about the good/service than the Principal/buyer
  2. The Principal/buyer has no viable way of verifying that the Agent/service has respected the "contract"

• If the market offers no ways of addressing information asymmetry, "good" principals/agents will be pushed out of the market

A practical example on used cars

• You want to buy a used car, go to two dealerships to check models and prices

<table>
<thead>
<tr>
<th></th>
<th>Dealership A</th>
<th>Dealership B</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Engine</strong></td>
<td>2000cc Gasoline</td>
<td>2000cc Gasoline</td>
</tr>
<tr>
<td><strong>Km</strong></td>
<td>200,000</td>
<td>150,000</td>
</tr>
<tr>
<td><strong>Mechanical problems</strong></td>
<td>Clutch will need replacement in 10k km</td>
<td>None</td>
</tr>
<tr>
<td><strong>Color</strong></td>
<td>Black</td>
<td>Black</td>
</tr>
<tr>
<td><strong>Internals</strong></td>
<td>Leather, good conditions</td>
<td>Leather, good conditions</td>
</tr>
<tr>
<td><strong>Price</strong></td>
<td>20,000E all incl.</td>
<td>18,000E all incl.</td>
</tr>
<tr>
<td><strong>Listing value</strong></td>
<td>15,000E</td>
<td>17,000E</td>
</tr>
</tbody>
</table>
A practical example on used cars

- Now consider you are a car expert with deep understanding of car mechanics & insurance
- Same cars as before! But NOW you know:

<table>
<thead>
<tr>
<th>Dealership A</th>
<th>Dealership B</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Engine</strong></td>
<td>2000cc Gasoline</td>
</tr>
<tr>
<td><strong>Km</strong></td>
<td>200,000</td>
</tr>
<tr>
<td><strong>Mechanical problems</strong></td>
<td>Clutch will need replacement in 10k km</td>
</tr>
<tr>
<td><strong>Color</strong></td>
<td>Black</td>
</tr>
<tr>
<td><strong>Internals</strong></td>
<td>Leather, good conditions</td>
</tr>
<tr>
<td><strong>Price</strong></td>
<td>20,000E all incl.</td>
</tr>
<tr>
<td><strong>Listing value</strong></td>
<td>15,000E</td>
</tr>
</tbody>
</table>

Not for sharing - Dr. Luca Allodi (TU/e) – Underground cybercrime economics

Adverse selection and moral hazard

<table>
<thead>
<tr>
<th>Adverse selection</th>
<th>Moral hazard</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What happens</strong></td>
<td>The buyer or the seller change their behavior after the contract is signed, effectively degrading previously obtained information</td>
</tr>
<tr>
<td>1. The buyer cannot evaluate the characteristics of the good and/or of the seller (seller has more information)</td>
<td></td>
</tr>
<tr>
<td>2. The seller cannot evaluate the characteristics of the buyer (buyer has more information)</td>
<td></td>
</tr>
<tr>
<td><strong>Examples</strong></td>
<td>The buyer fears that they’ll buy the “wrong” malware → either take the risk (at a premium) or quit the trade</td>
</tr>
<tr>
<td>1. Malware service provider stops delivering customer payload after payment</td>
<td>1. Buyer of insurance starts assuming unsafe behaviour after the contract is signed (as they are now risk neutral)</td>
</tr>
<tr>
<td>2. The seller cannot assess the past history of purchases from the buyer → sells cocaine to the Europol</td>
<td>2. Buyer of insurance starts assuming unsafe behaviour after the contract is signed (as they are now risk neutral)</td>
</tr>
</tbody>
</table>
Addressing info asymm. in criminal markets

• Cybercrime markets started off as a *scam-the-scammer* model
  • Mostly on IRC channels
  • Credit cards, banking info, “digital goods”, ..
    • Fundamental problem: as virtually all interactions are criminal, enforcing contracts is very hard
      → if you get scammed, you can’t go to the Interpol and report the “crime”..

• Two cases
  • Forum-based markets → where most of the malware is traded
  • E-commerce like markets → for drugs, weapons, other physical goods

Why malware → forums?

• Malware is a *niche* market
  • Despite much noise in media & literature it is relatively small in size
    • (in terms of number of actors and when compared to other illegal markets, e.g. drug)
    • Vulnerability finding and exploit engineering are highly complex tasks
    • Repeated trade is limited

• Large problems with adverse selection & moral hazard
  • How to evaluate an exploit or a malware?
    • Very difficult to test without giving it away

• Adverse selection
  • Tends to have extended technical discussions on workings of the attack
  • Technical details allow selection of attack that matches buyer needs (e.g. vulnerable sw versions, exploit reliability, ..)

• Moral hazard
  • Closed-access forums can enforce durable contracts (e.g. service-based malware provision)
Why drugs/illegal goods → e-commerce?

• Large(r) markets
  • Customers tend to “come back” to circle of trusted vendors
  • Non-technical goods, as long as they provide the “kick” they are good enough
  • Delivery times, costs, convenience over technical complexity
  • Repeated purchases create rich feedback history for buyers and sellers

• Anonymity is key factor
  • Physical delivery is especially vulnerable
  • Don’t want to expose one’s identity on clearnet
  • Quick entry / exit from the market reduces exposure

Forum markets
Forum markets of malware: mechanisms

- 2011-2013 → infiltrated several English+Russian speaking markets for malware and exploits
- Market evaluation:

<table>
<thead>
<tr>
<th>Market mechanism</th>
<th>Evidence</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moral hazard</td>
<td>Fear of punishment</td>
<td>Trials, active discussion, hinders unfair behavior</td>
</tr>
<tr>
<td></td>
<td>High cost of entry</td>
<td>Being banned is expensive</td>
</tr>
<tr>
<td></td>
<td>History of trade</td>
<td>Backs up seller’s trustworthiness / quality of goods</td>
</tr>
<tr>
<td></td>
<td>Reputation system</td>
<td>Reputation levels match punishment</td>
</tr>
<tr>
<td>Adverse selection</td>
<td>Product samples</td>
<td>Sellers provide tests, trials, videos of the exploit in operation for buyer to assess</td>
</tr>
<tr>
<td>Feedback mechanisms</td>
<td></td>
<td>Products are reviewed by buyers, positive/negative feedback</td>
</tr>
</tbody>
</table>

Moral hazard: user reputation

Bad market

![Bad market graph](image1)

Working market

![Working market graph](image2)

Not for sharing - Dr. Luca Allodi (TU/e) – Underground cybercrime economics
Moral hazard: rule enforcement (bad market)

- Market statement: trustworthy traders are in elite section
- Rules to access elite section of market
  1. More than 150 posts AND
  2. More than 4 months since registration
- Users consistently access “Tier 2” market with less than 150 posts and less than 4 months of operation
- Trust mechanism goes “down the pipe”
  - Rippers have access to “good” section of market as much as “trustworthy” users
  - Ineffective mechanism to enforce trade trust

Moral hazard: rule enforcement (working market)

- Market statement: untrustworthy players are up for trial
- Trial rules:
  1. Defender has from 24hrs up to 7 days to show up
  2. Evidence must be provided from both sides to support case
  3. Collective punishment for "guilty" players

Consistently enforced by market admins

<table>
<thead>
<tr>
<th>Case</th>
<th>Challenged amount</th>
<th>#Users involved</th>
<th>Evidence</th>
<th>#Messages</th>
<th>Duration</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defender no show</td>
<td>3906</td>
<td>7</td>
<td>Screenshots, transaction logs, chat transcripts, screenshots.</td>
<td>11</td>
<td>7 days</td>
<td>Defender banned</td>
</tr>
<tr>
<td>Defender loses</td>
<td>2800$</td>
<td>7</td>
<td>Screenshots, transaction logs, chat transcripts.</td>
<td>29</td>
<td>29 days</td>
<td>Defender banned</td>
</tr>
<tr>
<td>Defender wins</td>
<td>1400$</td>
<td>3</td>
<td>Chat transcripts, screenshots.</td>
<td>9</td>
<td>11 days</td>
<td>Defender found not guilty, no action taken</td>
</tr>
</tbody>
</table>

Trial regulation is strictly enforced. Evidence brought in support to the case of either the defender or the accuser is always critically analyzed; more controversial trials require longer time to be concluded, and the final decision can be in favor of either participant, depending on how convincing the evidence supporting one’s case was.
Trial: Collective punishment

- Payment of 3000 USD not received;
  - defender is given 12 hours to show up
- Defender shows up after 4 hours
  - Brings evidence of payment (very long discussion)
    - Posts logs & screenshots of transaction
- Accuser answers that the payment has never been received
  - He/She accuses the defender to have “blocked” or “intercepted” the payment
  - Witnesses on his side show up to support his claims and trustworthiness
- Admin gives two options
  - 1) Defender must provide final proof of transaction commit
  - 2) Defender and Accuser resolve the case in private
→ after a month of discussion the defendant hasn’t provided conclusive evidence
→ he ends up “in the Black” (i.e. listed as an offender)

Trial: Fear of punishment

- Accuser reports a failure on the defender’s side to close a transaction
- Reports transcript of their conversation
  - Accuser pays defender while the latter was offline
  - Defender does not acknowledge the payment
- Defender shows up, says he/she talked to the accuser and all is settled
- Accuser replies
  - “Have lost your mind?! Whom did you talk to??”
- Admin gives 24 hours to do “moneyback”
- Accuser declares:
  - Money returned - I have no claims
- Trial is closed and the defender is cleaned from any accusation
Proof of “moneyback”

Adverse selection: Example of trade of an exploit kit

Kit success rate → *success rates depend on quality of traffic

- Malware delivery rates
  - Zeus malware: 50-60%
  - Loader: 80-90%

- Latest prices
- Additional services

Contact
Monday – Saturday
From 7am to 5pm
Moscow Time
Adverse selection: Example of trade of a standalone exploit:

- 1-day Local priv. escalation exploit CVE-2016-7255 [XP-W10,x86 / x64]
- Vulnerability: CVE-2016-7255 (Published: November 8, 2016)
- [...] The following Windows protections are bypassed:
  - SMEP, Kernel DEP, KASLR, Integrity Level (out from Low), UAC, ...
- The exploit is delivered as a shellcode, ready to be embedded in your projects.
- The package includes demo source code that opens the command console with SYSTEM rights.
- Price 5000USD

Payment services

- Either direct payment or simple escrowing are adopted in forum markets
- The market mechanisms play a distinctive role in regulating fair behavior
- The role of administrators and moderators is a key enabler
  - Weakly enforced rules destroy trust in platform and ultimately lead to market collapse
  - Consistency and fairness of trial mechanisms is key
- Functioning market → competition
- Competition → technological innovation (==new vulns, new malware)
  - Without this, the cybercrime ecosystem for malware could collapse
“E-commerce” illegal markets

.onion services

- Illegal large underground markets are generally run as hidden services in the TOR network
- Assure **network** anonymity of both
  - The market admin — server
  - The market participants
- Actual anonymity can only be granted by appropriate **OPSEC**
  - Clearnet calls from JS/Flash/other plugins
  - People publishing their pub/sec key pairs on the markets
  - Host compromise leads to leaks
TOR: a quick recap

Chris Zachor “Anonymizing Network Technologies”

TOR in action (1)

Not for sharing - Dr. Luca Allodi (TU/e) – Underground cybercrime economics
TOR in action (2)

How Tor Works: 2

Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

Tor node
\[\text{encrypted link}\]
\[\text{unsigned link}\]

Alice

Jane

Bob

Dave

TOR in action (3)

How Tor Works: 3

Step 3: If the user wants access to another site, Alice's Tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

Tor node
\[\text{encrypted link}\]
\[\text{unsigned link}\]

Alice

Jane

Bob

Dave
TOR in detail

- Alice (OP) negotiate a key with every OR
- Every OR only knows who is before and after it
  - OR3 knows that the message is for Bob but does not know Alice sent it

How onion services work

This + next five slides from: https://www.torproject.org/docs/onion-services.html.en
Onion Services: Step 2

Step 2: Bob advertises his service -- XYZ.onion -- at the database.

Onion service descriptor

Onion Services: Step 3

Step 3: Alice hears that XYZ onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.

Alice obtains descriptor starting from .onion address
**Onion Services: Step 4**

Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.

**Onion Services: Step 5**

Step 5: Bob connects to the Alice’s rendezvous point and provides her one-time secret.
Onion Services: Step 6

Step 6: Bob and Alice proceed to use their Tor circuits like normal.

Not for sharing - Dr. Luca Allodi (TU/e) – Underground cybercrime economics
Feedback (1)

- Vendor levels, rating
- Vendor description
- Reviews
- Full list of items
- ...

Feedback (2)

Contact vendor

Username: LordOfTheGreen (3) (5.00★)
FE enabled: No
Join date: 04/09/2018
Last active: 03/12/2018 (today)

Trust?

3 3 3

Profile Ratings

<table>
<thead>
<tr>
<th>Age</th>
<th>1 Stars</th>
<th>2 Stars</th>
<th>3 Stars</th>
<th>4 Stars</th>
<th>5 Stars</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Newer than 1 Month</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3 (5.00★)</td>
</tr>
<tr>
<td>Newer than 3 Months</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>--</td>
</tr>
<tr>
<td>Older</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>--</td>
</tr>
</tbody>
</table>

Do not open links from ratings, they will contain phishing links. Phishing links are leading to fake websites which are stealing your login data.

Whaooooo!!! those guys are legit. Crazy good stealht, never seen anything like it before and the buds are very good, one joint put me on the moon!! Only point is that you don't get 'kind' you received so it would be nice to have it written on the package.

Great offer, 3y

Good come from vendor. FE'd in good faith, will update once product arrives.

3d 5

b...2 ~ $0.005

d...T ~ $0.005

4d 5

S...r ~ $0.005
Escrow services

Multi-sig escrow
Stand-alone markets

Finalize Early

- Some vendors can ask buyers to pay immediately
- Generally only “highly trusted” vendors are allowed access to this option
- The decision is taken by the market platform
- No clear effect on vendor trust/expected revenues
The case of arms dealing

- Market is relatively small
  - But so is the real-world underground market for illegal weapons
- Delivery
  - Multiple shipments of different components of weapon
  - Drop points where the weapons are and the buyer goes over to pick up

- Mostly small and light weapons
  - Guns
  - Semi-automatic
  - Explosives
- No missiles, chemical weapons, or highly destructive material
Some shipping details

**Our web address is: **
Check it before ordering. If in doubt, email

**Watch out for clone sites that steal your bitcoin:**

Thank you for choosing us for your own needs. We have a large selection of guns and equipment for you to choose from. All of our guns and equipment are brand new and have been checked thoroughly for defects. We want you to feel safe when you’re purchasing from us.

We ship all of our items with FedEx Standard Overnight within USA and FedEx International Priority for countries outside of USA. All shipping costs are free – as we have already added any shipping.

All of our guns are brand new and 100% gun oil free. So it takes custom without any issue. Handguns are taken apart and shipped inside copertin case or other item. All purchases come with instruction for assembling and maintaining your equipment. Due to the openness of this website, we cannot disclose example of the package.

---

Reading list

