Malware excellence: an example for contrast

Malware in an open “Deep web” marketplace

- **Vendor**: 01DigitalDiscount10
- **Price**: $20,000 (54.15)
- **Ships to**: Worldwide
- **Ships from**: Worldwide
- **Escrow**: Yes

Malware on an “invite-only” forum marketplace

- **Product description**: 
  
  This is a guide on how to hack into bank accounts using the Zeus bot. This does not come with the bot.
  
  **About Zeus**:
  
  Zeus, also known as Zeus, is a Trojan horse malware package that runs on versions of Microsoft Windows. While it can be used to carry out many malicious and criminal tasks, it is often used to steal banking information.

(Here was a screenshot with a very detailed exploit ad including vulnerability characteristics, execution time, evasion)
Social Eng. excellence: an example for contrast

From my spam folder
The classic “webmail problem, click here”

Multi-stage campaign targeting “white-collar” workers on LinkedIn

Characterizing excellence in...

Malware criminal endeavours
Can Dmitry sell his malware kit anywhere?

- Admin role, rule enforcement, (feared) punishment
- Coherent signals (e.g. reputation), aligned incentives
- Evidence of trade
- User-to-user feedback
- Product info, demos, trials

**Principles**

- Dispute resolution
- Reputation systems
- Interaction and information exchange
- Moral hazard
- Adverse selection

**Illustrative examples**

<table>
<thead>
<tr>
<th>Probably not-that-interesting forum market</th>
<th>Probably interesting forum market</th>
<th>Interesting ecrime platform</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="" /></td>
<td><img src="image2" alt="" /></td>
<td><img src="image3" alt="" /></td>
</tr>
</tbody>
</table>

**Coherent signals**

- [Box plot 1]
- [Box plot 2]
**Illustrative examples**

<table>
<thead>
<tr>
<th></th>
<th>Probably not-that-interesting forum market</th>
<th>Probably interesting forum market</th>
<th>Interesting ecrime platform</th>
</tr>
</thead>
</table>

**Coherent signals**

<table>
<thead>
<tr>
<th></th>
<th>Regulation (log)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>100</td>
</tr>
</tbody>
</table>

Rule enforcement outcomes

Rule: access tier 2 after 4 months
### Illustrative examples

<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>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defender no show</td>
<td>2800S</td>
<td>7</td>
<td>Chat transcripts, screenshots, transaction logs, chat transcripts, screen shots.</td>
<td>11</td>
<td>7 days</td>
<td>Defender banned</td>
<td>Defender never showed up.</td>
</tr>
<tr>
<td>Defender wins</td>
<td>1400S</td>
<td>3</td>
<td></td>
<td>29</td>
<td>29 days</td>
<td>Defender banned</td>
<td>Defender did not provide exhaustive evidence that the payment was ultimately committed in favor of the accuser. The defender demonstrated that goods were not delivered because the payment happened during a technical malfunction of his internet connection, and he therefore could not acknowledge it.</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.

**Rule:** access tier 2 after 4 months

---

**Evidence that participants initiating a trade also often declare to have performed a background check on the seller by either contacting the administrators or by checking the official blacklist of the forum.**

*e.g.,* "The admin [of the forum] confirmed me that you [the seller] are not a rookie trader.”

---

**User-to-user feedback & evidence of trade**
### Illustrative examples

<table>
<thead>
<tr>
<th>Probably not-that-interesting forum market</th>
<th>Probably interesting forum market</th>
<th>Interesting ecrime platform</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Image" /></td>
<td><img src="image2.png" alt="Image" /></td>
<td><img src="image3.png" alt="Image" /></td>
</tr>
</tbody>
</table>

1. **Illustrative examples**
   - **Probably not-that-interesting forum market**
     - ![Image](image1.png)
     - ![Image](image2.png)
     - ![Image](image3.png)

2. **User-to-user feedback & evidence of trade**
   - ![Image](image1.png)
   - ![Image](image2.png)
   - ![Image](image3.png)

---

**User-to-user feedback & evidence of trade**

- **Probably not-that-interesting forum market**
  - ![Image](image1.png)
  - ![Image](image2.png)
  - ![Image](image3.png)

- **Probably interesting forum market**
  - ![Image](image1.png)
  - ![Image](image2.png)
  - ![Image](image3.png)

- **Interesting ecrime platform**
  - ![Image](image1.png)
  - ![Image](image2.png)
  - ![Image](image3.png)
Why all the trouble?

• Usually threat ID comes “after the fact”
  1. Measure activity “in the wild”
  2. Derive corresponding threat model
  3. Identify market/community/criminal initiative that enables it
  4. Take (disruptive) action (sinkhole, jamming, LE actions, ..)

• If we know how to look selectively, we can go the other way around
  • Find the credible “La La Lands” and take selective and pre-emptive action

Example of application

• Investigation of the IMPaaS.ru criminal platform
  • IMPaaS.ru is a Russian closed access ecrime platform emerged in Dec’17
    • This platform implements a new model to obtain and distribute bundles of stolen credentials and user fingerprints to cybercriminals
  • Counting 260k+ stolen user profiles at time of infiltration

We infiltrated this market and studied the new threat model that emerges from it
Reconstructing attack operations from multiple sources

(1) Market observation
- Detailed product description
- Profile selection, enforcement
- Support infrastructure
- Provides a basis to be confirmed

(2) Affiliated underground communities
- Existent foothold in high profile markets
- User-to-user feedback
- Market confirmation
- Discussion of activities

(3) Infection campaign reports
- Industry reports aligned with malware doc
- Reported phishing campaigns vs malware
- Confirms profile acquisition details

(4) Malware replication
- Malware analysis supports functional claims
- Confirms profile acquisition details

(5) Market interactions
- Discussion in affiliated communities
- Telegram channels
- Evidence of product acquisition
- Discussion on employment
- Responsive admin

The Impersonation-as-a-Service (IMPaaS) model
Characterizing IMPaaS in the wild – distribution

Amount of profiles available per country

Median price per profile per country in USD

Characterizing IMPaaS in the wild – pricing

Moving weekly average price of stolen profiles

Price of profile vs country GDP

Some details:
- Prices range from 0.7 USD to 96 USD
- MNYTRANSF/CRYPTO + 6-10USD over expected price (+150%)
- SOCIAL, SERVICES, COMMERCE not highly valued

Observationally:
- Recent new infra development related to increase in mean price (+15USD)
- Pricing structure remained similar.