Some preliminary analysis of the economics of malware kits and traffic brokers

Workshop on “Collaborative Security and Privacy Technologies”

Luca Allodi, Fabio Massacci

25 April 2012, Berlin
Malware Markets

• Initially markets mainly traded goods such as
  – CCNs
  – SSNs
  – Bank accounts
• Initially took place on IRC channels
  – No proper moderation
  – No reputation system
  – It was a market for “Lemons”¹
• No ROIs → This paradigm failed

New Malware Markets

- Forums/e-commerce sites
- New features
  - Reputation Systems
  - Brokerage of tools
  - Infrastructure of services
    - Additional services to support the tools
  - “Language restricted” markets
- Feature the characteristics of a typical growing market
Who the attackers were, and are

- ’90s: hackers were security enthusiasts with high technical competence
- ’00s: hacker was anybody that could run an automated tool
- ‘10s: hackers are economic agents that look toward ROIs
  - Automation tools are not enough now
  - Trade of infrastructure
    - Exploit Kits
    - Traffic Brokers
Exploit Kits and Traffic Brokers

• Exploit kits are **web applications** deployed on some server
  – MySQL back-end
  – When the user connects to its `exploit.php` page
    • Exploit kit **test** victim’s configuration for known vulnerabilities -> exploit
    • Shellcode usually initiate download of some **malware**

• Problem
  ➢ The attackers needs the user to explicitly make a **GET** request toward `exploit.php`

• Solution
  ➢ **Buy connections** from Traffic Brokers
How Exploit Kits work

Hacker/Exploit kit owner

Exploit Kit

Points to

iFrame

Popular website homepage

User
How Exploit Kits work

Hacker/Exploit kit owner

Exploit Kit

Points to

Popular website homepage

User

iFrame

attacks
How Exploit Kits work

Hacker/Exploit kit owner → iFrame → Popular website homepage → User

Exploit Kit

Points to

attacks
How Exploit Kits are sold

Exploitation success rate
*Rate highly depends on traffic quality

Install rates
Zeus malware: 50-60%
Loader: 80-90%

Latest prices

Additional services

Vendor’s contacts

Working hours:
• Monday-Saturday
• 7am to 5pm (Moscow time)
How traffic redirection works

Exploit kit owner

Exploit Kit

Popular website homepage

iFrame

ADs

Traffic Broker / Hacker

User

attacks
How traffic redirection works

Exploit kit owner

Exploit Kit

iFrame

Popular website homepage

ADs

Traffic Broker / Hacker

User

Traffic redirection attacks
How traffic redirection works

Exploit kit owner

Exploit Kit

Exploit kit owner

Popular website homepage

iFrame

ADs

Traffic Broker / Hacker

User

Traffic attacks
How traffic redirection works

- Exploit kit owner
- Exploit Kit
- iFrame
- ADs
- Popular website homepage
- Traffic Broker / Hacker
- User
- Traffic redirection works
How traffic redirection works

Exploit kit owner

Exploit Kit

User

Traffic Broker / Hacker

ADs

iFrame

Popular website homepage

Buys traffic

attacks
How traffic redirection works

Exploit kit owner

Exploit Kit

Traffic Broker / Hacker

User

Popular website homepage

iFrame

ADs

Buys traffic

Attacks
How traffic redirection works

Exploit kit owner

Exploit Kit

Popular website homepage

ADs

iFrame

Traffic Broker / Hacker

User

Buys traffic

attacks

attacks
How traffic is sold

- Cybercrooks **buy** traffic from other crooks or online services (Ads network)

- **High traffic quality** means the cybercrook gets connections from the vulnerable systems he/she was looking for
Some math

- Cyber crook wants to build a 1 million bots botnet

<table>
<thead>
<tr>
<th>Action</th>
<th>Economic effort (1st year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buy exploit kit (20% efficiency)</td>
<td>2000 USD</td>
</tr>
<tr>
<td>Number of needed connections</td>
<td>5 x 10^6</td>
</tr>
<tr>
<td>Deployment</td>
<td>50-150 USD</td>
</tr>
<tr>
<td>Buy Traffic (assuming 2USD/1k)</td>
<td>10.000 USD</td>
</tr>
<tr>
<td>Maintain (change IPs, clear logs..)</td>
<td>150 USD</td>
</tr>
<tr>
<td>Updates (assume 2/yr)</td>
<td>~ 200 USD</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>~ 12.400 USD – 12.500 USD</td>
</tr>
<tr>
<td><strong>Breakeven ROI/BOT</strong></td>
<td>~ 0.01 USD</td>
</tr>
</tbody>
</table>
Thanks!

Any questions?