• My students of the Offensive Computer Security course please come meet me during the interval
“Hacker” evolution

<table>
<thead>
<tr>
<th>Attacker type</th>
<th>Emergence period (roughly)</th>
<th>Activity</th>
<th>Goals</th>
<th>Example of notable threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security enthusiasts</td>
<td>1990s → onwards</td>
<td>Innovate threats</td>
<td>Improving security, security testing, software evaluation, hardware flaws</td>
<td>Mitnick attack, Morris worm, ARP poisoning, social engineering, ..</td>
</tr>
<tr>
<td>Economic attacker</td>
<td>2010 → onwards</td>
<td>Innovative threats, delivery at scale, malware economy</td>
<td>Data exfiltration (CCNs, banking, accounts, ..), computational power, ransomware</td>
<td>Ransomware, exploit kits, payload obfuscation, malvertising, fast-flux, botnets, ..</td>
</tr>
</tbody>
</table>

The emergence of an underground economy

- From a “one-do-it-all” business model to a “composite” model
- Complexity and scale of attacks too big to have profitability if attacker has to:
  1. Identify victims
  2. Build infrastructure
  3. Develop attack (malware, phishing,..)
  4. Distribute payload
  5. Collect infections
  6. Monetize
  7. ..
- Product composition
  - Not a single entity covers *all* aspects
  - Cybercriminal composes the activity by relying on multiple services
  - Affiliate program can be however complex, technical or organizational
Cybercrime commoditization vs specialization

- Commoditization happens when products/consumer needs are largely undifferentiated
  - Sellers can come up with a service/good that can reach a wide set of potential customers
- Type of business models (Kurt 2015)
  - Spam
  - Extortion
  - Clickfraud
  - Social eng/fraud
  - Mining
  - Carding/Accouts

Spam to sell counterfeit products

- Spam techniques are used to advertise products
  - Stolen email accounts
  - Social networks
  - Mobile phones / calls..
- Victim is tricked into buying some counterfeit goods
  - Pharmaceutical / electronics / clothes..
  - Pirated software
  - Pornography, gambling, ...
- Sometimes the customer willingly look for these products
  - Competitive pricing + effective social engineering techniques
- Est. value between 60-90M depending on product
Ransomware

- Mix Social engineering + technical attack
- Substituted “scareware”/FakeAV campaigns
- Malware encrypts file on hard disk
  - Asks for money to give decryption key
  - Usually in the whereabouts of 100-200 $, up to 400 $.
  - Ransoms may vary depending on country
- Estimated value (CryptoLocker alone): ~ 3 Million USD
Click fraud

• Attacker registers with Ad Network
• Use infected systems to generate clicks on sourced advertisement
• Hard to distinguish between legitimate and fake click
  • Manual workers
  • Automated bots that do the clicking
  • Malware that hijacks actual user clicks
• Estimated 20% of all clicks are generated by automatic bots
  • Detection rate up to 75%
• Estimated value ~ 20-30 million USD

Other fraud models: Finance and banking

• “pump and dump”
  • Buy cheap stocks from “over the counter” markets
    • E.g. Pink market in the “OTC markets group”
  • Use SE to convince victims in buying more stocks → inflate price
  • Resell original stock, bubble deflates, gain 4-5% on initial investment
• Credit cards, banking → hard to cash-out
  • Obtain cards through skimming, malware
  • Hard to resell, same cards shared among several buyers
Scareware

- Uses a combination of social engineering and malware infection
- Convinces user they need to buy a product
  - FakeAV is typical example
- Message convinces user system is infected or at risk
  - Typically pay about 60$ to get the system “cleaned”
- Common threat before 2011
- Estimated value 130 million USD
  - Market dismantled by blocking transactions to FakeAV affiliate programs

Not for sharing - Dr. Luca Allodi - Cyber attacks and defenses - Underground economics

Boothe services


Not for sharing - Dr. Luca Allodi - Cyber attacks and defenses - Underground economics
Exploit-as-a-service and PPIs

- Platforms to deliver malware
  - Self-replicating malware is not attractive for monetization
  - Hard or impossible to control propagation → high visibility, visible effects
- Full infrastructure that
  - Selects potential targets with specific characteristics
    - E.g. Windows system running in Brazil using IE 9
  - Redirects victims to an “exploit kit”
  - Drops malware
- PPI → pre-infected machines with “droppers”
  - Pay-Per-Install
  - Class of malware whose function is to install arbitrary malware

Revenue examples

<table>
<thead>
<tr>
<th>Profit Center</th>
<th>Strategy</th>
<th>Estimated Revenue</th>
<th>Time Frame</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software &amp; Ransomware</td>
<td>Fake anti-virus [133]</td>
<td>$1.30 million</td>
<td>2008–2010</td>
</tr>
<tr>
<td></td>
<td>CryptoLocker [159]*</td>
<td>$3 million</td>
<td>2013–2014</td>
</tr>
<tr>
<td></td>
<td>DNS Changer [149]*</td>
<td>$14 million</td>
<td>2007–2011</td>
</tr>
<tr>
<td>Financial Scams</td>
<td>Pump and dump [150]*</td>
<td>$1.20 million</td>
<td>2008–2013</td>
</tr>
<tr>
<td></td>
<td>419 scammers [8]*</td>
<td>$200 million</td>
<td>2006</td>
</tr>
<tr>
<td>Credit Card Theft</td>
<td>ATM withdrawal scam [118]*</td>
<td>$45 million</td>
<td>1 day</td>
</tr>
<tr>
<td></td>
<td>Zeus banking Trojan [9]*</td>
<td>$70 million</td>
<td>2009–2010</td>
</tr>
<tr>
<td></td>
<td>Re-selling stolen cards [35]*</td>
<td>$300 million</td>
<td>7–2013</td>
</tr>
</tbody>
</table>

Table 1: Estimated revenue from a multitude of profit strategies (irrespective of operating costs). These strategies span the spectrum of cybercrime: from selling illegal products to outright credit theft. We annotate all industry and government estimates of criminal revenue with an asterisk to emphasize an unknown collection methodology. We caution these values may be overestimates.
Revenues vs ransomware

<table>
<thead>
<tr>
<th>Family</th>
<th>Addresses</th>
<th>BTC</th>
<th>USD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locky</td>
<td>6,827</td>
<td>15,399.01</td>
<td>7,834,737</td>
</tr>
<tr>
<td>CryptXXX</td>
<td>1,304</td>
<td>3,339.68</td>
<td>1,878,696</td>
</tr>
<tr>
<td>DMALockerv3</td>
<td>147</td>
<td>1,505.78</td>
<td>1,500,630</td>
</tr>
<tr>
<td>SamSam</td>
<td>43</td>
<td>632.01</td>
<td>599,687</td>
</tr>
<tr>
<td>CryptoLocker</td>
<td>944</td>
<td>1,511.71</td>
<td>519,991</td>
</tr>
<tr>
<td>GlobelImposter</td>
<td>1</td>
<td>96.94</td>
<td>116,014</td>
</tr>
<tr>
<td>WannaCry</td>
<td>6</td>
<td>55.34</td>
<td>102,703</td>
</tr>
<tr>
<td>CryptoTorLocker2015</td>
<td>94</td>
<td>246.32</td>
<td>67,221</td>
</tr>
<tr>
<td>APT</td>
<td>2</td>
<td>36.07</td>
<td>31,971</td>
</tr>
<tr>
<td>NoobCrypt</td>
<td>17</td>
<td>54.34</td>
<td>25,080</td>
</tr>
<tr>
<td>Globe</td>
<td>49</td>
<td>33.03</td>
<td>24,319</td>
</tr>
<tr>
<td>Globev3</td>
<td>18</td>
<td>14.34</td>
<td>16,008</td>
</tr>
<tr>
<td>EDA2</td>
<td>23</td>
<td>7.1</td>
<td>15,111</td>
</tr>
<tr>
<td>NotPetya</td>
<td>1</td>
<td>4.39</td>
<td>11,458</td>
</tr>
<tr>
<td>Rasy</td>
<td>1</td>
<td>10.75</td>
<td>8,073</td>
</tr>
</tbody>
</table>


Monetisation

- Selling attacks for a price is not enough to justify the market
- It must be possible to “monetise” the traded technology
  - Several mechanisms to monetise infections are possible
- Largely based on money mules
  - Act as a relay for ban/money transfers, with the promise of retaining a compensation
  - Receive and re-send expensive goods used to convert stolen credit to merchandise
- Full monetization process for all activities is still unclear
  - Some may just be ponzi-scheme-like settings
Case study on exploit kits

- Exploit kits are websites that serve vulnerability exploits and ultimately to malware
- Affect client side vulnerabilities
- Drop malware upon successful exploitation  
  - Fully customizable
- Typically feature <10 exploits  
  - Trend is decreasing in time  
  - Now many exploit kits feature 3-4 exploits

Baseline workings
Baseline workings

This is the GET response. Can't remove it without breaking the web

This is the original GET request

User

Attacks

Third party traffic

• Exploit kits only work if they receive victim traffic
  • Direct links, ads, iframes, redirections, ..
• Underground has services that trade connections
  • “Maladvertising”, spam, iframes on legit websites
• Attacker “buys” connections from specific users, with specific configurations
  • Javascript checks local configuration
  • Sends to remote server
  • Remote server redirects to exploit kit
  • User loads the webpage the attacker compromised, and if characteristics match traffic is redirected
Exploit kits: advanced

Exploit kits: actual
Kits’ defensive components

Crawler aware (6)
IP Blocking (26)
Obfuscation (27)
Neither Obfuscation nor IP Blocking (2)

Ekit interaction: Crimepack
Details on attacks

Define and inject exploit and shellcode
Administer

Exploit selection
Drive-by attacks “in the wild”

Dependencies and activity types
Deep web and cybercrime commoditization
Deep web and cybercrime commoditization

Details of an ad

- No real technology, just a “manual”
- Out for 4-5$`
- Looking for malware and exploits leads essentially only to porn (13/12/18)
  - Clearly not a malware / exploit repo
  - Most to consume “second grade” hacking products
    - See first class for distinction
Market size & type of cybercrime products

- Lots of listings
  - Botnet → renting
  - Exploit → Office macros
  - Malware → Ransomware
- 30% of listings in B2B
- 45% of listings in B2C
- No qualitative evaluation of products

<table>
<thead>
<tr>
<th>Market</th>
<th># Listings</th>
<th># Vendors</th>
<th>Total revenue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agorà</td>
<td>3,240</td>
<td>526</td>
<td>$1,818,991</td>
</tr>
<tr>
<td>Alphabay</td>
<td>21,350</td>
<td>3,055</td>
<td>$13,471,406</td>
</tr>
<tr>
<td>Black Market Reloaded</td>
<td>2,069</td>
<td>386</td>
<td>$685,108</td>
</tr>
<tr>
<td>Evolution</td>
<td>9,551</td>
<td>1,002</td>
<td>$6,125,136</td>
</tr>
<tr>
<td>Hydra</td>
<td>377</td>
<td>28</td>
<td>$242,220</td>
</tr>
<tr>
<td>Pandora</td>
<td>1,204</td>
<td>169</td>
<td>$394,306</td>
</tr>
<tr>
<td>Silk Road 1</td>
<td>4,053</td>
<td>645</td>
<td>$2,239,436</td>
</tr>
<tr>
<td>Silk Road 2</td>
<td>2,734</td>
<td>441</td>
<td>$4,455,339</td>
</tr>
</tbody>
</table>

Vendor distributions and product pricing

<table>
<thead>
<tr>
<th>Category</th>
<th>Listings per vendor</th>
<th>Revenue per listing</th>
<th>Price per listing</th>
<th>Lifespan in months</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Median</td>
<td>Mean</td>
<td>Median</td>
<td>Mean</td>
</tr>
<tr>
<td>App</td>
<td>1</td>
<td>1.97</td>
<td>$24.33</td>
<td>$5.70</td>
</tr>
<tr>
<td>Botnet</td>
<td>1</td>
<td>1.61</td>
<td>$34.44</td>
<td>$14.73</td>
</tr>
<tr>
<td>Cash-out</td>
<td>2</td>
<td>5.88</td>
<td>$60.00</td>
<td>$14.85</td>
</tr>
<tr>
<td>E-mail</td>
<td>1</td>
<td>2.58</td>
<td>$22.85</td>
<td>$7.34</td>
</tr>
<tr>
<td>Exploit</td>
<td>1</td>
<td>1.56</td>
<td>$15.57</td>
<td>$5.26</td>
</tr>
<tr>
<td>Hosting</td>
<td>1</td>
<td>1.33</td>
<td>$31.60</td>
<td>$16.40</td>
</tr>
<tr>
<td>Malware</td>
<td>1</td>
<td>1.95</td>
<td>$22.90</td>
<td>$5.45</td>
</tr>
<tr>
<td>Phone</td>
<td>1</td>
<td>1.80</td>
<td>$30.00</td>
<td>$9.90</td>
</tr>
<tr>
<td>RAT</td>
<td>1</td>
<td>1.66</td>
<td>$20.00</td>
<td>$5.41</td>
</tr>
<tr>
<td>Website</td>
<td>1</td>
<td>2.28</td>
<td>$29.80</td>
<td>$8.72</td>
</tr>
</tbody>
</table>
Revenue by product in time

With cash-outs (e.g. CVVs)

Without cash-outs

Specialized market; market organization

- Several “themes”
  - [Вирусология] → Virusologia → malware, exploits, packs, ...
  - [Доступы] → Access → FTP Servers, shells, SQL-i, ...
  - [Серверы] → Servers → VPN, proxies, VPS, hosting, ...
  - [Социальные сети] → Social networks → accounts, groups, ...
  - [Спам] → Spam → emailing, databases, mail dumps, ...
  - [Траф] → Internet traffic → connections, iframes, ...
  - [Финансы] → finance → bank accounts, money exchange, ...
  - [Работа] → Work → look up for and offer jobs
  - [Разное] → other
Top 10 on “virusologia”

- Exploit Kit “RIG v3”
- Tool to encrypt malware
- Exploit Kit “Neutrino”
- Sale of Office exploits
- Dropper “Nuclear” (EKit)
- Kernel exploits for Windows
- Crypt online service
- Web attacks injector
- Malware bots

MALWARE

- Capabilities:
  - 1. Work around NAT
  - 2. Written in C++
  - 3. Hidden installation

- Full support for Windows XP \ Vista \ 7 \ 8 \ 8.1 \ 10 x86-64 as well as server systems
- [...] (redacted)
- 19. Escalation of privileges (CVE 2015-1701)
- 20. UrlDownloader
  - ✓ Small size (31kb)
  - ✓ Does not interact with UAC and firewall
  - ✓ Crypt by third-party cryptors without my intervention

- 22. Spawns only one process. The name and description are custom.
  - Languages supported: Russian, English, Arabic, Chinese, Czech, Danish, Dutch, French, German, Hebrew, Italian, Japanese, Korean, Norwegian, Polish, Portuguese-Brazilian, Spanish, Swedish, Turkish

- Price: 4000USD
Details of an EKIT ad

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

Ransomware

• 1. 61 kb (UPX - 24 kb);
• 2. Multi-threaded file encryption;
• 3. New algorithm based on AES-256 using RSA-2048
• 4. You can set prices based on country
• 5. Handy ticket system
• ...
• 12. Infection disabled for these countries: AM AZ BY GE KG KZ MD RU TJ TM UA UZ [CSI];
• ...
• 1. No price, get 50% of revenue.
• 2. Absolutely do not touch CSI countries.
• 3. Instant payments
• ...
Mobile bots

Real App

Injected page

Price: 4000$ lifetime updates

Market activity: sellers

- Number of (exploit) vendors is growing at a steady rate
- Most present on market for 1yrs at time of first exploit sale
- Exploit introduction
  - EKIT → 4-10/author
  - STDALONE → 3-6/author
Package prices

<table>
<thead>
<tr>
<th>Type</th>
<th>n</th>
<th>Min</th>
<th>0.025p</th>
<th>Mean</th>
<th>Median</th>
<th>0.975p</th>
<th>Max</th>
<th>sd</th>
<th>Min</th>
<th>0.025p</th>
<th>Mean</th>
<th>Median</th>
<th>0.975p</th>
<th>Max</th>
<th>sd</th>
</tr>
</thead>
<tbody>
<tr>
<td>EKIT</td>
<td>6</td>
<td>150</td>
<td>157.92</td>
<td>693.89</td>
<td>400</td>
<td>1875</td>
<td>2000</td>
<td>708.94</td>
<td>2</td>
<td>2.12</td>
<td>6.83</td>
<td>7</td>
<td>11</td>
<td>11</td>
<td>4.26</td>
</tr>
<tr>
<td>MALWARE</td>
<td>6</td>
<td>420</td>
<td>428.75</td>
<td>1735</td>
<td>1250</td>
<td>3875</td>
<td>4000</td>
<td>1456.38</td>
<td>1</td>
<td>1</td>
<td>1.5</td>
<td>1</td>
<td>2.88</td>
<td>3</td>
<td>0.84</td>
</tr>
<tr>
<td>STANDALONE</td>
<td>26</td>
<td>100</td>
<td>100</td>
<td>2972.69</td>
<td>3000</td>
<td>8000</td>
<td>8000</td>
<td>2629.99</td>
<td>1</td>
<td>1</td>
<td>1.5</td>
<td>1</td>
<td>4</td>
<td>4</td>
<td>0.86</td>
</tr>
<tr>
<td>All</td>
<td>38</td>
<td>100</td>
<td>100</td>
<td>2417.46</td>
<td>1500</td>
<td>8000</td>
<td>8000</td>
<td>2408.28</td>
<td>1</td>
<td>1</td>
<td>2.34</td>
<td>1</td>
<td>11</td>
<td>11</td>
<td>2.63</td>
</tr>
</tbody>
</table>

- EKIt's business model allows vendors to keep low prices for on average more exploits than other packs
  - 2-11 exploits per pack
  - Prices are shrinking with new releases
  - High market interest (expl.as.a.service)
- STDL by far the most expensive, >3000USD
  - 1-3 exploits per pack
  - Prices inflating
- MALWARE is midway, few exploits
  - Prices inflating

Exploit age at market introduction

- STANDALONE arrive the fastest
  - Most within 6 months
  - Fastest 2.5% within a week
  - Slowest 2.5% more than 1.5yrs
  - Matches higher price tag
- EKITs much slower on average
  - Most within 1 yr
- Exploit vendors are becoming faster at introducing new exploits
  - Approx rate of 30%/yr
Exploit trends

![Graph showing exploit trends over years with data points for Adobe, Microsoft, and Oracle.

**Exploits no more! Firefox 26 blocks all Java plugins by default**

Click-to-run activated even for latest version.

By Felix McAlister in San Francisco © Dec. 2013

Not for sharing - Dr. Luca Allodi - Cyber attacks and defenses - Underground economics

Exploit (re) introduction

- Slow rate of exploit introduction, >6mnths
- Most re-packs start from STDL

<table>
<thead>
<tr>
<th>CVE</th>
<th>no.</th>
<th>Sw</th>
<th>SwVendor</th>
<th>Type 1</th>
<th>Type 2</th>
<th>Type 3</th>
<th>Type 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-8651</td>
<td>4</td>
<td>flash</td>
<td>adobe</td>
<td>STANDALONE</td>
<td>STANDALONE</td>
<td>STANDALONE</td>
<td>EXIT</td>
</tr>
<tr>
<td>2010-0188</td>
<td>4</td>
<td>acrobat</td>
<td>adobe</td>
<td>EXIT</td>
<td>EXIT</td>
<td>MALWARE</td>
<td>MALWARE</td>
</tr>
<tr>
<td>2012-1864</td>
<td>3</td>
<td>windows</td>
<td>microsoft</td>
<td>STANDALONE</td>
<td>MALWARE</td>
<td>MALWARE</td>
<td>MALWARE</td>
</tr>
<tr>
<td>2015-1701</td>
<td>3</td>
<td>windows</td>
<td>microsoft</td>
<td>STANDALONE</td>
<td>MALWARE</td>
<td>MALWARE</td>
<td>MALWARE</td>
</tr>
<tr>
<td>2010-4452</td>
<td>3</td>
<td>java</td>
<td>oracle</td>
<td>EXIT</td>
<td>EXIT</td>
<td>STANDALONE</td>
<td>EXIT</td>
</tr>
<tr>
<td>2006-0003</td>
<td>3</td>
<td>int.expl.</td>
<td>microsoft</td>
<td>EXIT</td>
<td>EXIT</td>
<td>EXIT</td>
<td>EXIT</td>
</tr>
<tr>
<td>2010-1885</td>
<td>3</td>
<td>windows</td>
<td>microsoft</td>
<td>EXIT</td>
<td>EXIT</td>
<td>EXIT</td>
<td>EXIT</td>
</tr>
<tr>
<td>2016-1019</td>
<td>2</td>
<td>flash</td>
<td>adobe</td>
<td>STANDALONE</td>
<td>EXIT</td>
<td>STANDALONE</td>
<td>EXIT</td>
</tr>
<tr>
<td>2015-2729</td>
<td>2</td>
<td>acrobat</td>
<td>adobe</td>
<td>STANDALONE</td>
<td>STANDALONE</td>
<td>STANDALONE</td>
<td>EXIT</td>
</tr>
<tr>
<td>2013-0640</td>
<td>2</td>
<td>acrobat</td>
<td>adobe</td>
<td>STANDALONE</td>
<td>STANDALONE</td>
<td>STANDALONE</td>
<td>EXIT</td>
</tr>
<tr>
<td>2015-2545</td>
<td>2</td>
<td>office</td>
<td>microsoft</td>
<td>STANDALONE</td>
<td>STANDALONE</td>
<td>STANDALONE</td>
<td>STANDALONE</td>
</tr>
<tr>
<td>2015-0057</td>
<td>2</td>
<td>windows</td>
<td>microsoft</td>
<td>STANDALONE</td>
<td>STANDALONE</td>
<td>MALWARE</td>
<td>STANDALONE</td>
</tr>
<tr>
<td>2013-3660</td>
<td>2</td>
<td>windows</td>
<td>microsoft</td>
<td>STANDALONE</td>
<td>STANDALONE</td>
<td>MALWARE</td>
<td>EXIT</td>
</tr>
<tr>
<td>2011-0611</td>
<td>2</td>
<td>acrobat</td>
<td>adobe</td>
<td>EXIT</td>
<td>EXIT</td>
<td>STANDALONE</td>
<td>EXIT</td>
</tr>
<tr>
<td>2010-0866</td>
<td>2</td>
<td>java</td>
<td>oracle</td>
<td>STANDALONE</td>
<td>EXIT</td>
<td>STANDALONE</td>
<td>EXIT</td>
</tr>
<tr>
<td>2006-2463</td>
<td>2</td>
<td>office</td>
<td>microsoft</td>
<td>EXIT</td>
<td>EXIT</td>
<td>STANDALONE</td>
<td>EXIT</td>
</tr>
<tr>
<td>2015-0336</td>
<td>2</td>
<td>flash</td>
<td>adobe</td>
<td>EXIT</td>
<td>EXIT</td>
<td>STANDALONE</td>
<td>EXIT</td>
</tr>
<tr>
<td>2013-3918</td>
<td>2</td>
<td>int.expl.</td>
<td>microsoft</td>
<td>STANDALONE</td>
<td>STANDALONE</td>
<td>STANDALONE</td>
<td>EXIT</td>
</tr>
<tr>
<td>2015-2419</td>
<td>2</td>
<td>int.expl.</td>
<td>microsoft</td>
<td>STANDALONE</td>
<td>STANDALONE</td>
<td>STANDALONE</td>
<td>EXIT</td>
</tr>
<tr>
<td>2014-6332</td>
<td>2</td>
<td>windows</td>
<td>microsoft</td>
<td>EXIT</td>
<td>STANDALONE</td>
<td>EXIT</td>
<td>STANDALONE</td>
</tr>
<tr>
<td>2010-0840</td>
<td>2</td>
<td>java</td>
<td>oracle</td>
<td>STANDALONE</td>
<td>EXIT</td>
<td>STANDALONE</td>
<td>EXIT</td>
</tr>
<tr>
<td>2011-3544</td>
<td>2</td>
<td>java</td>
<td>oracle</td>
<td>STANDALONE</td>
<td>EXIT</td>
<td>STANDALONE</td>
<td>EXIT</td>
</tr>
<tr>
<td>2012-0158</td>
<td>2</td>
<td>office</td>
<td>microsoft</td>
<td>STANDALONE</td>
<td>EXIT</td>
<td>STANDALONE</td>
<td>STANDALONE</td>
</tr>
</tbody>
</table>
Exploits “À la carte”

Excerpt of (bootstrapped) exploit prices in the underground market

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Software</th>
<th>Min</th>
<th>0.005p</th>
<th>Mean</th>
<th>Median</th>
<th>0.015p</th>
<th>Max</th>
<th>ad</th>
<th>n</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft</td>
<td>Office</td>
<td>150</td>
<td>150</td>
<td>2801.82</td>
<td>2250</td>
<td>1000</td>
<td>1000</td>
<td>2993.49</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td></td>
<td>150</td>
<td>150</td>
<td>2442.13</td>
<td>2450</td>
<td>5400</td>
<td>5600</td>
<td>1601.69</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>150</td>
<td>150</td>
<td>3195.45</td>
<td>4000</td>
<td>7250</td>
<td>8000</td>
<td>2304.34</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>150</td>
<td>150</td>
<td>2947.31</td>
<td>2862.5</td>
<td>5759</td>
<td>8000</td>
<td>(1132.54)</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Int. expl.</td>
<td>640</td>
<td>459.5</td>
<td>3035</td>
<td>1850</td>
<td>7025</td>
<td>8000</td>
<td>3504.22</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>440</td>
<td>440</td>
<td>3921.85</td>
<td>3000</td>
<td>8000</td>
<td>8000</td>
<td>(1272.18)</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Windows</td>
<td>700</td>
<td>800</td>
<td>2366.67</td>
<td>2250</td>
<td>4875.5</td>
<td>5000</td>
<td>1458.34</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>700</td>
<td>1100</td>
<td>(2394.07)</td>
<td>(2372.27)</td>
<td>(2375.09)</td>
<td>8000</td>
<td>(658.77)</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Silverlight</td>
<td>150</td>
<td>150</td>
<td>150</td>
<td>150</td>
<td>150</td>
<td>150</td>
<td>(1)</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>150</td>
<td>150</td>
<td>150</td>
<td>150</td>
<td>150</td>
<td>150</td>
<td>(150)</td>
<td>(150)</td>
</tr>
</tbody>
</table>

Not for sharing - Dr. Luca Allodi - Cyber attacks and defenses - Underground economics

(a) Chrome (Finifter et al. Usenix 2013)

(b) Firefox

Selling traffic

• Can buy traffic from “traffic brokers”
  • User does not have to click on anything
  • Automatic redirect
• High-quality traffic derives from selection of connection based on requested criteria
  • Geographic source
  • Installed software
Infect 100k machines: is it worth it?

Let’s say you want to infect 100 thousand machines (medium-large botnet)

<table>
<thead>
<tr>
<th>Action</th>
<th>Cost (1st year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buy exploit kits (20% efficiency)</td>
<td>2,000 USD</td>
</tr>
<tr>
<td>Required connections</td>
<td>500,000</td>
</tr>
<tr>
<td>Setup</td>
<td>50-150 USD</td>
</tr>
<tr>
<td>Traffic (assuming 2USD/1000 conn.)</td>
<td>1,000 USD</td>
</tr>
<tr>
<td>Maintenance (IP/domain flux, packing..)</td>
<td>150 USD</td>
</tr>
<tr>
<td>Updates (assuming 2/yr)</td>
<td>200 USD</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>3,400 USD – 3,500 USD</strong></td>
</tr>
<tr>
<td><strong>Breakeven ROI/infection</strong></td>
<td><strong>0.03/0.04 USD</strong></td>
</tr>
</tbody>
</table>

Exploit kit internals

Technical and operational research @ Tu/e
Offensive components

• Delivers the attack
  1. Detects browser and operating system (88%)
  2. Checks system hasn’t been attacked yet (64%)
     • via IP checking
  3. Checks if system is actually vulnerable
     • Browser and plugin versions
  4. Launches appropriate attack
     • Less sophisticated kits launch the attack even if system isn’t sophisticated enough (36%)

• Exploits typically attack vulns on:
  • Adobe Flash, Acrobat Reader, Internet Explorer, Java, other plug-ins
Defensive components

- Many exploit kits **defend** themselves against AV/robot detection
- **Payload and malware obfuscation** (82%)
  - Obfuscation + crypto
  - Malware packers
- Block IP to avoid probes (78%)
- Evasion robots+crawlers
- Some check whether the domain on which the exploit kit is hosted is included in antimalware lists
Reading list


