Cybercrime in the Deep Web

Dr. Martin “Doc” Carlisle
Overview of online crime

Case studies
- Online sale of drug
- How FBI shut down Silk Road

Ongoing cyber crime examples
- IRS tax returns

Give you an idea of
- Different players involved in online crime
- Intervention strategies
Online crime

- Emergence of underground economy
  - Loose federation of specialists selling capabilities, services, and resources explicitly tailored to the abuse ecosystem

- Streamlines abuse – for a fee
  - Commoditization provides access to:
    - Compromised machinery
    - Sensitive user data
    - Human services
    - Accounts & engagement

  - Difficult for any single actor to extract all this value
Online crime – Profit centers

Flow of external capital into underground

Slide ack: Thomas Kurt
Online crime – Support centers

<table>
<thead>
<tr>
<th>Specialized Payloads</th>
<th>Spambot</th>
<th>Clickbots</th>
<th>Banking trojans</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Grum, Storm, MegaD</td>
<td>ZeroAccess</td>
<td>Zeus, SpyEye</td>
</tr>
<tr>
<td>Malware distribution</td>
<td>Exploit kits</td>
<td>PPI services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nuclear, Blackhole</td>
<td>GoldInstalls, Loader Adv</td>
<td></td>
</tr>
<tr>
<td>Traffic acquisition</td>
<td>Accounts</td>
<td>SEO, cloaking</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Email, social, phishing</td>
<td>Backlinks, websites</td>
<td></td>
</tr>
<tr>
<td>Raw materials</td>
<td>Hosting, networking</td>
<td>Human services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hosts, proxies, domains</td>
<td>Captcha, SMS, content, mules</td>
<td></td>
</tr>
</tbody>
</table>

Flow of capital into underground

Slide ack: Thomas Kurt
Case study: Online sale of drugs

- One of the best known illicit online trades
  - Who hasn’t received email spam for prescription drugs?

- Potentially most dangerous form of online crime
  - Wrong dosage can kill: cf. Ryan Haight

- Complex supply chain that can tell us a lot about the online criminal ecosystem
Supply chain: high-level overview

- Malware designer
- Malware installer
- Botnet operator
- Advertiser (spam, search-engine manipulation)
- Pharmacy store (website)
- Inventory owner (affiliate network operator)
- RX lab
- Payment processors

$ $ $ $ $ $
Advertising unlicensed drugs

- Malware designer
- Malware installer
- Botnet operator
- Advertiser (spam, search-engine manipulation)
- Pharmacy store (website)
- RX lab
- Inventory owner (affiliate network operator)
- Payment processors

$
Email spam has been the primary vector for a long time

Very low conversion rate* (about 1 purchase every 12.5 million emails sent for Rx)
Unsolicited

More recently: social network spam (e.g. Twitter)

Better conversion rate* (Twitter spam: 0.13%)
Posting malicious links via compromised accounts
Exploiting trust relationships

Search engine manipulation

Targeted to users looking for a product
Probably better conversion rates

*Ratio of realized sales over the number of emails/clicks
Original search-redirection attack (1)
[Leontiadis, Moore and Christin, USENIX Security 2011]
Only two of the results actually belong to online pharmacies. The rest are unrelated .com or .edu sites that had been compromised to redirect to online pharmacies or have been populated with spam.
Novel attack variants (2012+)

- **Ex.1 Inlining the store front in the compromised website**
  - A click then leads you to the pharmacy

- **Ex.2 Stateful server**

- **Goal:** escape detection by automated crawlers

- Attackers are quickly adapting to monitoring and/or countermeasures
- Non-trivial amount of effort on their part!
Questions

- **How has the attack evolved?**
  - Volume and impact
  - Techniques

- **Why has the attack evolved?**
  - Effectiveness of the defenses?

- **Can this be thwarted?**
  - Network-level intervention vs. end-host intervention
Attack modus operandi: Redirection chains

- Query executed
- Source infection(s)
- Redirector(s)
- Online pharmacies

- no prescription Cialis
- cs.umass.edu
- sylvan.k12.ca.us
- ...
- stat-center.com
- (or click)
- 302
- secureTabsOnline.com
- best-online-cialis-store.com
- genericTab.com
- genericRxPharma.com
- 302
Data collection process

Run 218 drug related queries daily.
• Daily collection from 4/12/2010 through 9/16/2013

Collect top 64 search results from Google
• The limit is defined by Google Search API
• Storing all results for later processing
• Will also examine position information

Identify all results that perform automated redirection
• A search result defines the website that a user will be redirected to when clicking on the link
• If the browser is redirected instead to a different website (domain), the result is infected.

Follow all infected results
• Follow each result identified as infected from previous step
• Follow all redirections that might occur
• Record all the redirection information
Datasets collected
[Leontiadis, Moore and Christin, ACM CCS 2014]

- **Dataset 1**
  - Aggregate results only
  - Rank of the results unknown
  - Mapping query-results unknown

- **Dataset 2**
  - Same as Dataset 1, but ranking information known
  - Mapping query-result doesn’t include rank

- **Dataset 3**
  - All information is captured
  - ... but Google started to limit what we could get

<table>
<thead>
<tr>
<th>Dataset</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Period</td>
<td>4/12/10-11/15/10</td>
<td>11/15/10-10/8/11</td>
<td>10/8/11-9/16/13</td>
</tr>
<tr>
<td>Search results/query</td>
<td>64</td>
<td>64</td>
<td>16/32</td>
</tr>
<tr>
<td>Total results</td>
<td>260,824</td>
<td>3,609,675</td>
<td>1,530,099</td>
</tr>
<tr>
<td>Unique URLs</td>
<td>150,955</td>
<td>189,023</td>
<td>122,382</td>
</tr>
<tr>
<td>Unique domains</td>
<td>25,182</td>
<td>36,557</td>
<td>30,881</td>
</tr>
</tbody>
</table>
Some of the 218 queries used

<table>
<thead>
<tr>
<th>Type</th>
<th>Count</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious (Black)</td>
<td>26</td>
<td>22%</td>
</tr>
<tr>
<td>Benign (White)</td>
<td>75</td>
<td>34%</td>
</tr>
<tr>
<td>Ambiguous (Gray)</td>
<td>117</td>
<td>54%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>218</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

vicodin no prescription  
cheap valium non prescription  
buy ativan online injecting pills  
buy xanax valium online florida  
order vicodin si levitra online  
buy xanax valium online florida  
color of adipex pills safest place to buy online

vicodin without prescription  
generic cialis free sample  
cheap tadalafil  
20 mg ambien overdose  
prozac side effects  
ambien buy online  
alprazolam online without prescription buy cheap
Dataset 1: 2010-2011

Search-redirection took over forum spam

Avg. daily domains in search results

- Infections
- Blog/forum spam
- Illicit pharmacies
- Health resources

Search redirection attack is rising

Blog spam is declining
Datasets 2: 2011-2013

Longitudinal evolution

Evolution of search results

G1: Google changes search ranking algorithm
G2: Google starts removing query info from “Referer” field
G3: Google is done deploying Referer modifications
B1, B2, B3: Firefox, Safari, Chrome switch to HTTPS-only search
(C1,C2: major changes to our collection infrastructure)
Uncovering relationships in search results

Search result (umass.edu)

Redirector (xorg.pl/...)

Pharmacy (menshealth-pharmacy.com)

Search result (bitbooks.com)

Redirector (f0e7.info)

Other pharmacy (megarxpills.com)
Possible interventions (network side)

Valuable infected sites (e.g., umass.edu)

Redirectors that could be targeted for removal

Pharmacies

* Results here are for 2010-2011
Evolution in concentration (1)

Maximum degree of traffic brokers and destinations over time

Average degree of traffic brokers and destinations over time
Despite changes in the actual hosts used, the network structure has remained relatively stable over time.

Large redirectors (traffic brokers) have only started to divest into smaller pieces in 2013.
Network infrastructure used by illicit advertisers

- Observed high concentration in traffic brokers
- Where are they located?

Traffic brokers observed each day grouped by AS

- # of redirection chains
  - 0
  - 200
  - 400
  - 600
  - 800

- 2012
- 2013

- US1
- US2
- US3
- DE1
- DE2
- DE3
- NL
- DE3
Effects of clean-up efforts (1)
Effects of clean-up efforts (2)

Survival probability over entire duration

- Source infections
- Traffic brokers
- Destinations

"Half life":

- 1 month
- 2.5 months
- > 3 months
Effects of clean-up efforts (source infections over time)

Median days before cleanup (overall)
Summary of measurement findings

- Search-result poisoning is here and has become a primary vector of advertisement

- Four-year longitudinal study shows
  - Little sign of abatement despite opportunities
  - Large concentration in traffic brokers, especially AS-level
  - Adaptivity of attackers to countermeasures
  - Clean-up time decreased at end-hosts but still large (1 month on average, still ~2 weeks+ in 2013)
Online criminal market place

- **A lot of dark market places**
  - Silk Road
  - Agora
  - Utopia
  - TheRealDeal
  - Alpha bay
  - ...

- **Early adopters of technology**
  - Tor hidden service
  - Bitcoin
Silk Road—Beginning

- **Jan 1, 2011**
  An unknown individual using the alias 'altoid' begins posting on internet forums shroomery.org and bitcointalk.org, advertising a hidden Tor service like an "anonymous amazon.com."

- **March 1, 2011**
  Messages on Bitcoin Talk: Silk Road has been operational for 3 weeks

- **April 11, 2011**
  Silk Road hits 1000 users
Oct. 11, 2011: Altoid Looks For a Bitcoin IT Pro

Bitcoin Talk user 'altoid' (alleged to be the same altoid who originally announced Silk Road's presence) posts a job ad for an "IT pro in the Bitcoin community" to work in a "venture-backed Bitcoin startup company". Interested parties are asked to write to "rossulbricht at gmail dot com." Allegedly, this post links 'altoid' to Ross Ulbricht, putting him under the authorities' suspicion.
Feb. 5, 2012: Dread Pirate Roberts
On Silk Road forums, user "Silk Road" announces "I need an identity separate from the site and the enterprise of which I am now only a part. I need a name. Drum roll please........ my new name is: Dread Pirate Roberts". This becomes the official forum mouthpiece for Silk Road.

Nov. 11, 2011: Dread Pirate Asks Stackoverflow For Tech Tips
Someone creates an account on programming advice site StackOverflow.com with the name 'Ross Ulbricht' and email address rossulbricht@gmail.com.

The curl script posted in the above Stack Overflow question is identical to code obtained from one of the Silk Road servers.
Silk Road—The End

- **July 23, 2013**
  The FBI Gets An Image of The Silk Road Server

- **July 24, 2013—July 31, 2013**
  Homeland Security Confronts Ulbricht

- **Oct. 1, 2013**
  Ulbricht is Arrested

- **Oct. 2, 2013**
  Silk Road Seized By Law Enforcement
  Bitcoin value crashes
  Vendors arrested
A subpoena to Google provided information about the accountholder

- details of IP addresses used to log into Mr. Ulbricht's account (San Francisco, specifically an internet cafe on Laguna Street)
- IP address is a VPN server

VPN server’s records were obtained by FBI

- VPN server's records indicated a user had accessed it from a San Francisco Internet café near the home of a friend Ulbricht had gone to live with

The FBI Gets An Image of The Silk Road Server

- hosting provider at the request of the FBI via local authorities and the Mutual Legal Assistance Treaty.
Silk Road—Gaps?

- FBI claimed it was because of a misconfiguration of the site's CAPTCHA, which inadvertently revealed Silk Road's IP address.
  - doubts about this claim
  - Someone claim the attack on Tor around the same time is related
New approaches

- Race to file tax returns
Ransomware

- Possible reuse of intelligence agency tools

Merck

@Merck

We confirm our company's computer network was compromised today as part of global hack. Other organizations have also been affected (1 of 2)

10:03 AM - Jun 27, 2017

28 replies 609 retweets 341 likes
More Ransomware

- **Colonial Pipeline Cyber Attack – May 7, 2021**
  - Paid $4.4 million ransom
  - Pipeline restarted after 5 days
  - FBI recovered 63.7/75 bitcoins of ransom

- **Meat supplier JBS – June 2021**
  - Paid $11M ransom
Takeaway

- Online crime is increasing in magnitude
  - Search-redirection for online pharmacies:
    - top 12 clusters account for 2/3 activity
    - Few, large, traffic brokers
  - Large number of participants perhaps induced by these “big shots”
    - This plays to the advantage of the defender!
    - Disrupt dependencies of the underground market

- Darknets
  - Use Tor hidden service
  - Police manage to collect enough information to shut down many
  - Top Tor Darknet Links 2021 to Visit

- New approaches being created