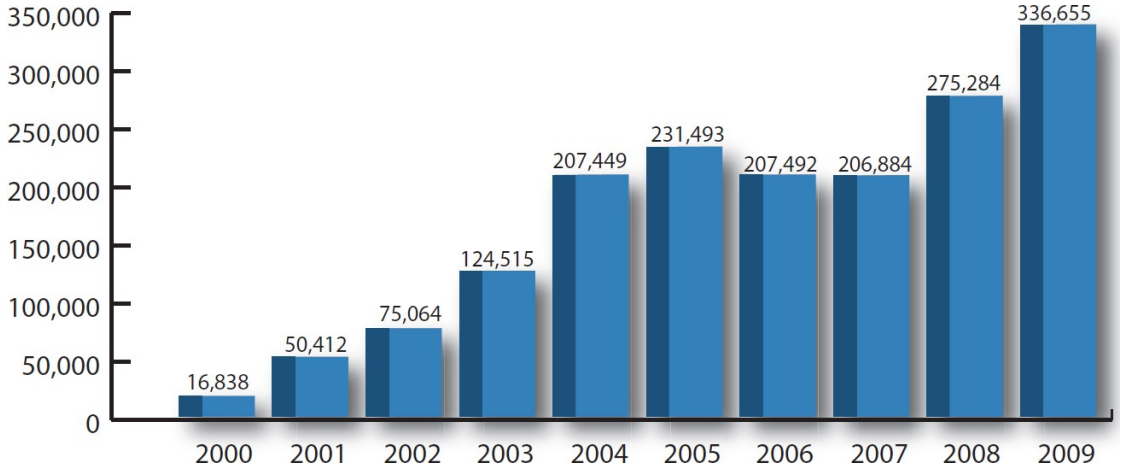
Covertly Probing Underground Economy Marketplaces

Hanno Fallmann, Gilbert Wondracek,
Christian Platzer

- Significant rise in criminal activity on the Internet



Received Complaints: IC3 Website [Internet Crime Report 2009]

- Cyber-criminals use online communication channels to coordinate themselves and to trade goods and services
- This enables them to specialize in the field of their expertise

- Researchers and law enforcement have a vital interest in acquiring data about the activities of underground economy marketplaces
- We present a novel system for **automatically identifying** and **covertly monitoring** a large number of underground marketplaces simultaneously
- Knowledge about the characteristics of these marketplaces is necessary

Underground Economy Marketplaces

- Most interesting marketplaces are
  - **IRC channels:** popular text-based chat protocol
  - **Web forums:** online discussion site
- Both marketplaces are actively policed

IRC (Internet Relay Chat)

- IRC networks use customized protocols to add new features, for example:
  - Limit on number of messages directed at different targets per time unit
  - Enable users to hide their real host address – “vhosting”
  - Primitive mechanism to check if user is human
  - Primitive check of user-client to thwart bots

IRC (Internet Relay Chat)

Web Forum

- Interesting content only visible for registered users
- Reputation-based systems and services:
  - Trading systems only accessible to members with a minimum reputation rating
  - Gain reputation by
    - Successfully performing business transactions
    - Contribute a certain amount of helpful posts
    - Payed a fee
  - Escrow services – forum administrators charge a fee to verify the goods

Credit Card Information

- Depending on the type of exploit the extend of information that must be known varies:
  - **Remote exploit**: using stolen information to order goods via Internet or telephone. Preferred are “cardable” shops.
  - **Creating a physical copy**: besides having the complete data of a card, a card printer and a hologram is required.
- The price for a card orients itself on the country of origin of the card holder, the type of the card, the volume of the content, and the exclusiveness of the information.

```
Sell Fresh US Cvv2 Visa / MasterCard 2.5$ Amex / Discover 4$
Sell US Fullz SSN+DOB+MMN 7$ ---
Sell WorldWide Proxy/Sock5 1$ Each -
Accept LibertyReserve & Perfect Money only. Msg me for deal!
```

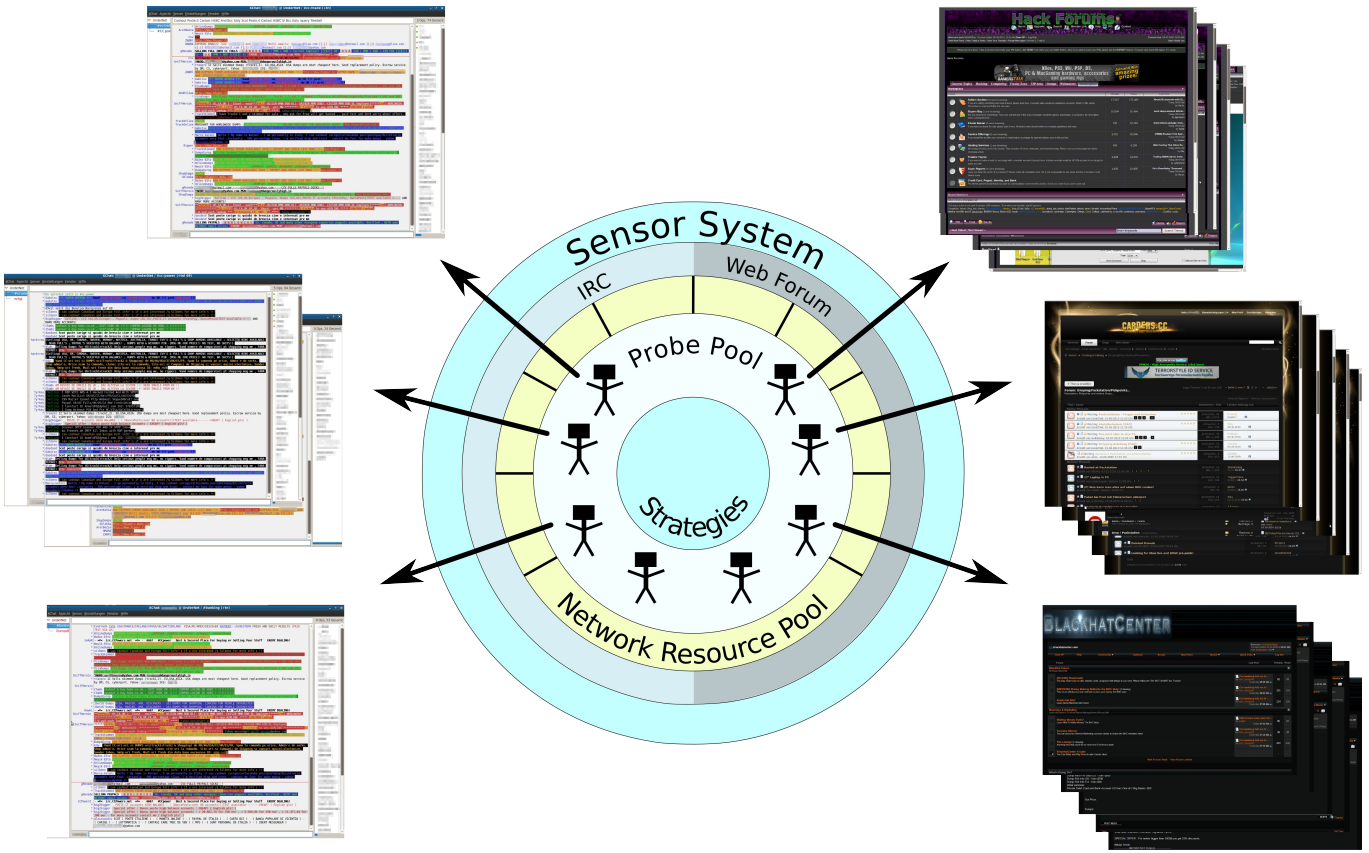
Other Goods and Services

- Malware
  - Malware programs and tool kits are being offered
  - Some even include support service
  - Boast with anti-detection mechanisms
- Identity Information
  - Provide stolen personal information: address, phone numbers, social security number
  - Complete Documents: passports, driver licenses, or transportation tickets
- Account Credentials: online games, file hosting services, or social websites

Underground Economy Advertisements

I offer serious DDoS attack service from 10 Gbps to 100 Gbps.
I always have between 80,000 and 120,000 bots on my IRC channel. Type of attack : SYN - TCP - ICMP - UDP - HTTP - HTTPS - NEWSYN
I can take down every website even if DDoS protected.
Price start from 200 $ USD 24 hours.
AVAILABLE : Free 3 minutes demonstration of attack.

Sensor System



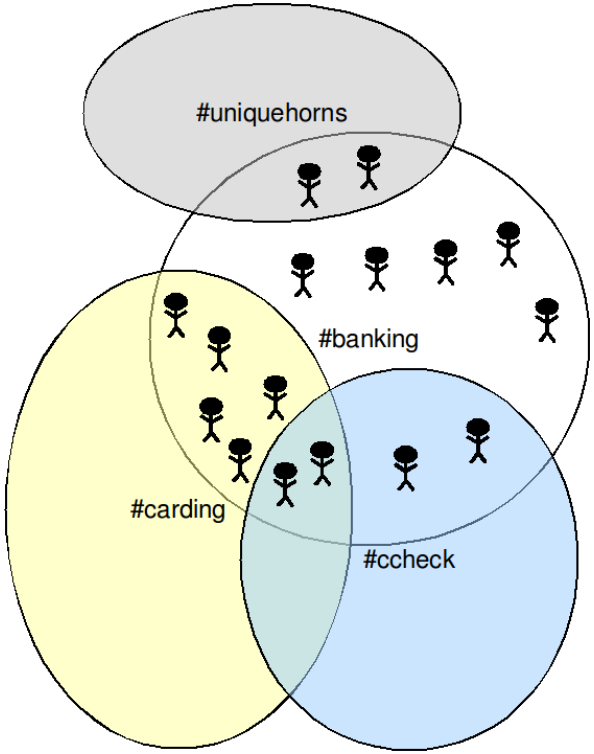
IRC Sensor: Monitoring Strategies

- Sensor Strategy

Channel	Include Patterns								Exclude Patterns				observe
	cvv	#cc-*	*trade*	*ccv*	*cashout*	*card*	*credit*	*verified*	*mp3*	*game*	*movie*	*video*	
#cc-trade		■	■										✓
#cc-power		■				■							✓
#onestopshop									■		■		×
#ccvalid				■									✓
#indocarder						■		■					✓
#Mp3traderz			■						■				×
#cvvcheck	■		■				■						✓
#tradewars			■							■			×
#drwho-central						■	■				■		×
#cashout					■			■					✓
#carding			■			■							✓
#TheCoop			■						■			■	×

IRC Sensor: Monitoring Strategies

- Chain Strategy
  - Extend the observation scope by joining unobserved popular channels
  - Determine which other channels users of #banking are currently joined by sending IRC whois requests
  - Join the most popular one (#carding) and apply the same strategy
  - Number of newly joined channels limited by configuration



IRC Sensor: Monitoring Strategies

- Chat strategy
  - Cyber-criminals post their advertisements via announcement-bots
  - Users are asked to request more detailed information
  - As soon as we recognize an invitation pattern, we engage the user in a private conversation using an artificial conversational system
  - System based on AIML (Artificial Intelligence Markup Language):
    Based on patterns, proper responses to incoming message are located

IRC Sensor Monitoring Strategies

Channel message:

```
Trader: #ccards :i need cvv, to trade it with gud leads,
                 if u have pm me
```

Private conversation:

```
Probe: sounds good, need more information too trade
Trader: jus need cvv fullz and i trade it with my leads
Probe: How badly do you need cvv fullz ? That is interesting.
Trader: i need it just to upgrade an account
Probe: "cvv fullz"? You need it to upgrade an account?
```

IRC Sensor: Monitoring Strategies

- Swap strategy
  - Passive users are frequently removed from IRC channels
  - Solution: after a period, we swap the probes with an intentional overlap time
- Combinations
  - By combining strategies and applying different observation methods we can construct new strategies

IRC Sensor: Information Gathering Methods

- CTCP (Client To Client Protocol)

```
FINGER jerry arthur (fraudster@mail.com) Idle 44861
seconds
VERSION mIRC v6.16 Khaled Mardam-Bey
USERINFO I'm a FBI's agent.
TIME Thu Aug 20 21:18:37 2009
```

IRC Sensor: Information Gathering Methods

- DCC (Direct Client to Client) Protocol
- IRC Whois

```
311 thedude jeff 192.168.178.1 * :Jeffrey Lebowski
317 xxcarderxx 31017 1253087663 :seconds idle, signon time
319 Manager :@#full @#Ccpower @#verifications @#CC2Bank
```

- IP Address Information
  - We can apply tools like Nmap, GeoIP, or blacklist lookups

IRC Sensor: Supervising Information Gathering

- Some of these strategies are conspicuous → have to be applied carefully

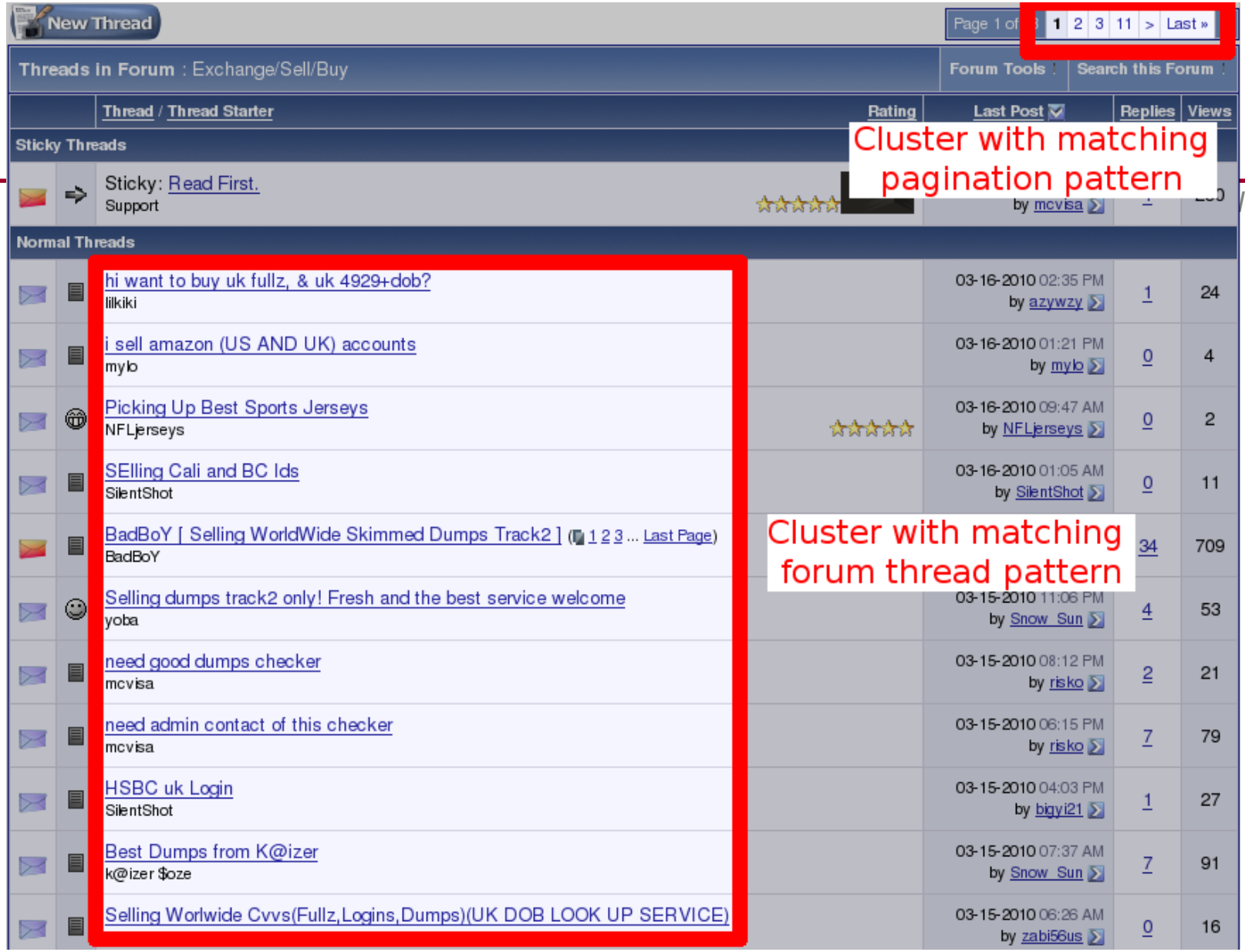
- Aim: Avoid causing nuisance or needless traffic
- Solution: Supervisor
  - Capable of recognizing affinity of channel to underground economy (Support Vector Machine)
  - Automatically dispatches fitting strategies and determines observation methods

IRC Sensor: Supervising Information Gathering

- Scanning an IRC network for fraudulent channels:
  - Sensor strategy: find obvious trading channels
  - Chain strategy: find neighboring popular channels
  - Randomly join channels

Web Forum Sensor

- Challenges of crawling a web forum:
  - Same content has multiple URIs (noisy links) → spider trap
  - Multitude of forum engines and versions → crawler has to be generic but still needs to be capable of recognizing structure
- Solution: crawling techniques described by Yang et al. [Extract Structured Data from Web Forums 2009]


New Thread
Page 1 of 3
1 2 3 11 > Last »
Threads in Forum : Exchange/Sell/Buy
Forum Tools
Search this Forum
Thread / Thread Starter
Rating
Last Post
Replies
Views
Cluster with matching pagination pattern
Sticky Threads
Sticky: Read First.
Support
by mcvisa
Normal Threads
hi want to buy uk fullz, & uk 4929+dob?
lilkiki
03-16-2010 02:35 PM
by azywzy
1
24
i sell amazon (US AND UK) accounts
mylo
03-16-2010 01:21 PM
by mylo
0
4
Picking Up Best Sports Jerseys
NFLjerseys
03-16-2010 09:47 AM
by NFLjerseys
0
2
SElling Cali and BC Ids
SilentShot
03-16-2010 01:05 AM
by SilentShot
0
11
BadBoY [Selling WorldWide Skimmed Dumps Track2] (1 2 3 ... Last Page)
BadBoY
34
709
Cluster with matching forum thread pattern
Selling dumps track2 only! Fresh and the best service welcome
yoba
03-15-2010 11:06 PM
by Snow_Sun
4
53
need good dumps checker
mcvisa
03-15-2010 08:12 PM
by risko
2
21
need admin contact of this checker
mcvisa
03-15-2010 06:15 PM
by risko
7
79
HSBC uk Login
SilentShot
03-15-2010 04:03 PM
by bigyi21
1
27
Best Dumps from K@izer
k@izer $oze
03-15-2010 07:37 AM
by Snow_Sun
7
91
Selling Worlwide Cvvs(Fullz,Logins,Dumps)(UK DOB LOOK UP SERVICE)
03-15-2010 06:26 AM
by zabi56us
0
16

Web Forum Sensor: By-passing Protections

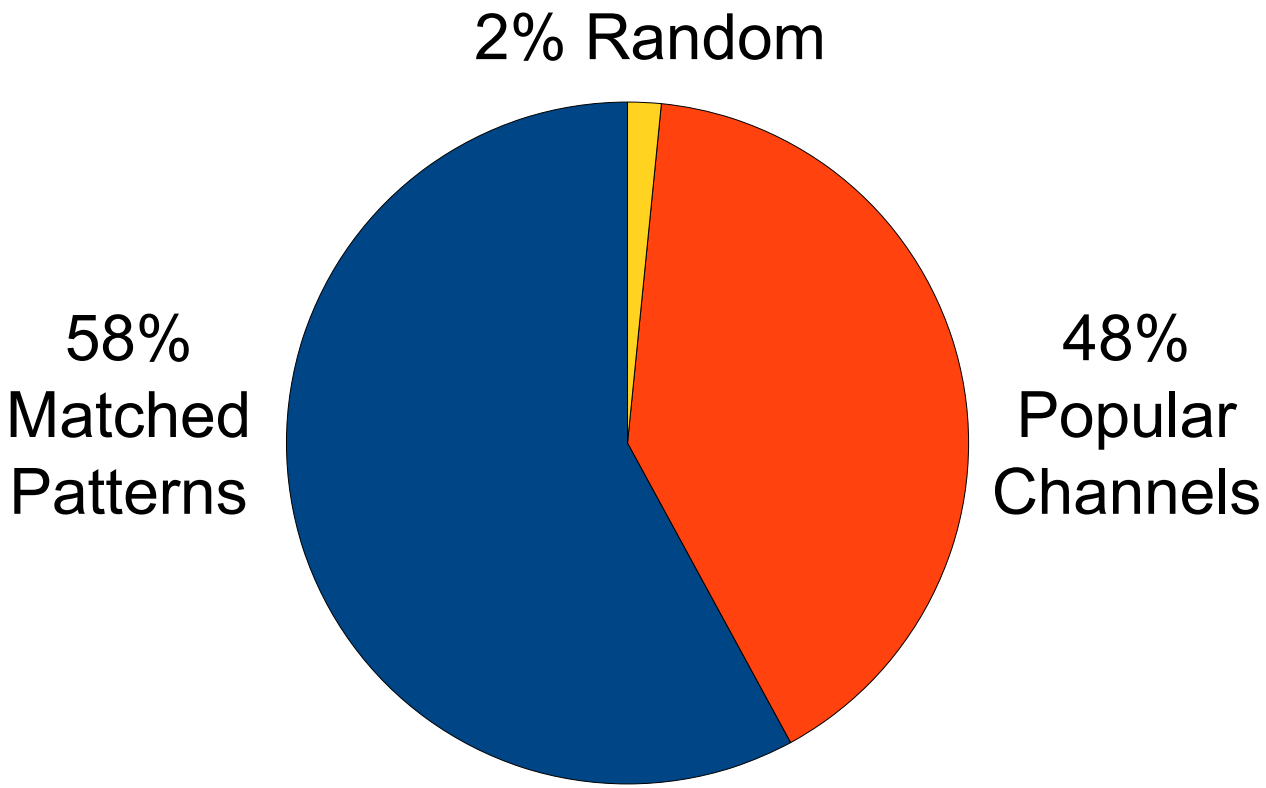
- Interesting content only available to registered users
  → create them manually
- Limited number of pages per time unit accessible
  → swap user accounts and network addresses

More stealth with distributed crawling

Evaluation

- Gathered data for a period of eleven months
- IRC Data:
  - We covered **291 IRC networks** and found over **495,000 distinct user names**
  - We observed over **26,000 IRC channels**
  - **126 channels** were recognized by the SVM to be underground economy trading channels
  - Chat system started **79 conversations**
  - **43 million messages** related to cyber-crime were recorded → **15 GB of data**

Evaluation: IRC Scanning Coverage



Evaluation: Web Forum

- Eleven underground forums have been thoroughly analyzed
- Recovered **one million posts** written by approximately **55,000 users** → **127 GB** of data
- Found three types of web forum usages by cyber-criminals:
  - Spamming legit forums
  - Discussion of crime related topics
  - Trading illegally obtained goods and offering questionable services

Questions?