

# Discussions in Deep, Dark, and Open: Monitoring the Social Discourse of Cyberattack

Oct 10, 2013

Jack Zaiantz, Bob Bechtel, Matt Hollingsworth

[Jzaiantz@soartech.com](mailto:Jzaiantz@soartech.com)

[bob.becht@soartech.com](mailto:bob.becht@soartech.com)



## SOARTECH

Modeling human reasoning.  
Enhancing human performance.

# Support cyberattack analysis through social discourse

- **What Needs to Be Done:** Provide cyber analysts with better tools for monitoring large social media streams by
  - detecting expected and unknown items of interest
  - detecting deliberate attempts to spread disinformation, incite hostilities, propagate cyberattack tools
  - assessing source quality
- **What's Hard:** We have a haystack, but are not sure that it's needles we're looking for
  - Difficult to detect unknown facts (new cyber-attack methods)
  - Difficult to manually develop filters that capture the complexity of the domain
  - Difficult to understand map of community boundaries relative to cyberattack development
- **What we're doing / Core Insight:**
  - Developing a search query grammar and associated filter algorithms and visualization tools to *leverage the innate linguistic and communication structure of social media*
- **Timeline:**
  - Have done initial experimentation under IRAD funds. Will be developing prototype interfaces and algorithms over next two years with goal of operational testing

Insight/hypothesis: Much as frequency analysis is a core cryptanalysis technique because it exploits known regularities in language, social discourse analysis can be a core technique in social media analysis because it exploits known regularities in language (including communications patterns, term use)

# Social Media as OSINT, both HUMINT and COMINT

- HUMINT – *direct observation, where sensor is secondary to observation*
  - Intentional or inadvertent “civilian sensors” with eyes on a situation
  - Comparing pre- and post- event social media behavior to gauge civilian reaction and attitudes
  - Disaster Impact and Battle Damage Assessment imagery

New Checking for the new SabPub malware in OS X <http://t.co/wU>

new malware version

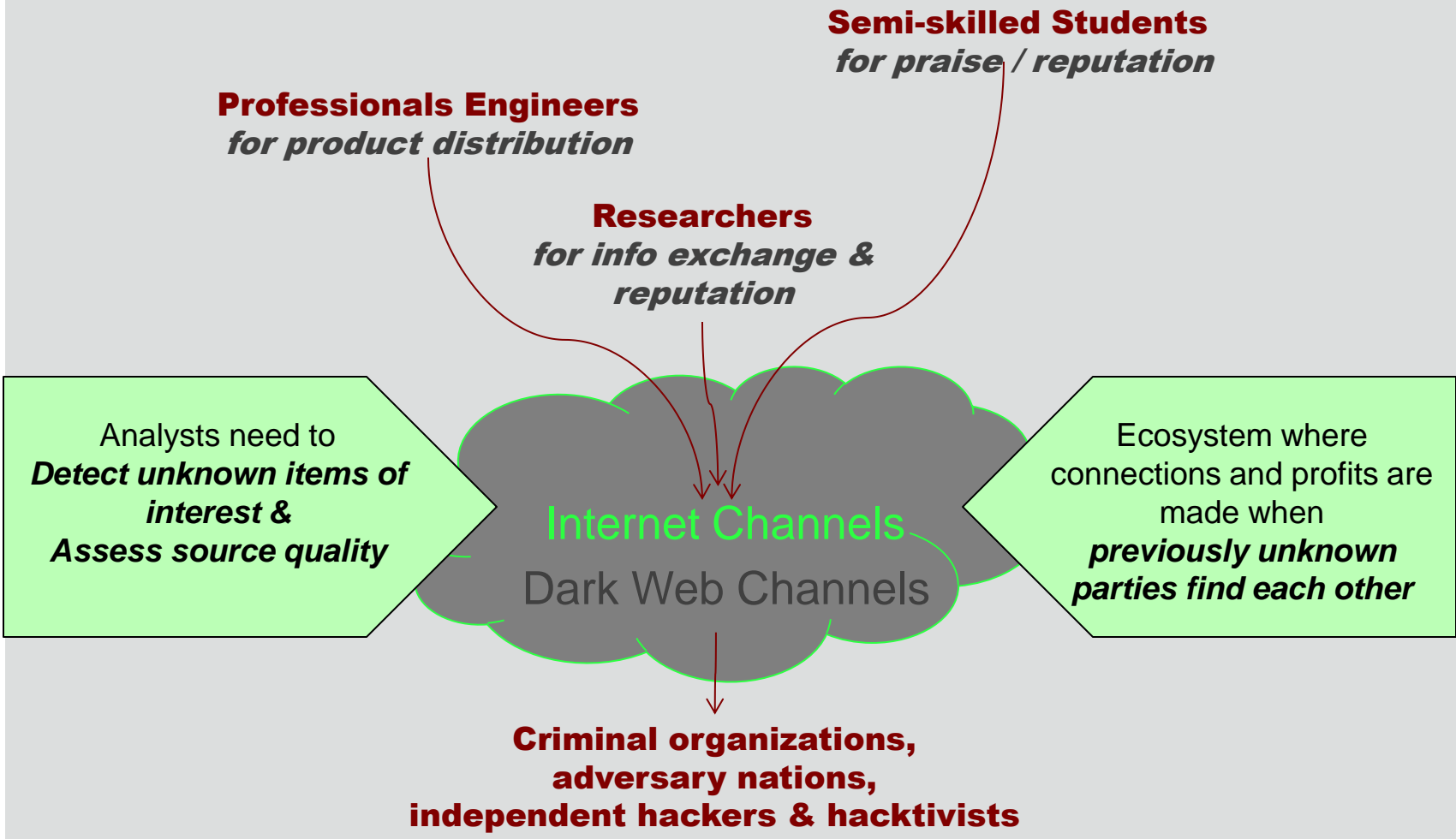
- COMINT – *intercepted communications, where sender/receiver is critical*
  - Adversarial influence operations & disinformation
  - Requests for support (HA/DR supplies, intervention)
  - Advertisement / movement of contraband (particularly cyber)
  - Claims of responsibility for attacks
  - Development of trans-national networks

New Checking for the new SabPub malware in OS X <http://t.co/wU>  
#occupycanada #occupytoronto #occupyvancouver  
#occupymiami #occupydc

“political  
hacktivists” are  
aware of new  
malware version

# CyberAttack communication in the open web

## Cyber Attack Tool Development



The internet is used by to facilitate communication between anonymous or previously unknown-to-each-other collaborators

# Monitoring social media for *communication*

- **Leveraging social media communication structure helps overcome big-data scaling issues**
  - but new end-user tools are needed...
- **Community-specific language:**
  - *Communities use specific terminology that can be used for filtering, but it's challenging to discover and results in combinatorics in filter definition*
- **Communication Patterns:**
  - *Communities use stable communication patterns ; e.g. novelty signaling, shouting/#beaconing*

## **Novelty Signaling**

Combine novelty & cyberattack terms

**Novelty:** new, novel, recent

**CyberAttack:** access control, adware, arbitrary memory, bot, botnet, brute force, buffer overflow, buffer size validation, cache poisoning, ddos ...

*Recent experiment used over 300 term pairs to filter 1 year of twitter fire-hose to less than 5 cyber-relative tweets per day.*

## **Twitter Shout**

Using multiple hashtags to make a tweet findable by target communities

**Adversaries, collaborators, and at-risk populations want to be found.  
But we need to be listening properly**

# More examples from the wild.....

**Webroot @Webroot** 30 May  
 New day, new DDoS for hire service. This one? Marijuana-themed & ready for cybercriminal consumption. [bit.ly/16tiDCs](http://bit.ly/16tiDCs) #ThreatBlog

**HackingAlert @HackingAlert** 28 Oct 11  
 ethical hacking: #RefRef - The new DDoS Tool By Anonymous [bit.ly/uzl72K](http://bit.ly/uzl72K)  
 Followed by DeScribe

**GLERINSON @glerinsonsec** 19  
 Hola anonymous,. arrivad new ddoS attack..... happy new year 2013 [pic.twitter.com/QPqias5INw](http://pic.twitter.com/QPqias5INw)

**WEBROOT® threat blog**  
 Products Support Community & Resources Partners About Webroot About the Bloggers

**Marijuana-themed DDoS for hire service sp in the wild**  
 Posted on May 30, 2013 by ddanchev  
 By Dancho Danchev

Largely thanks to the increasing availability of easy to use DIY (do-it-yourself) DDoS bots, we continue to see an increase in international cybercrime-friendly market propositions for 'DDoS for hire' services. And while these services can never match the bandwidth capabilities and vendor experience offered by their Russian and European counterparts, they continue to empower novice internet users with the ability to launch a DDoS attack against virtually anyone online.

In this post, I'll profile a recently launched marijuana-themed DDoS for hire service and emphasize on its built-in pseudo-anti-abuse process, the service is prone to be abused by novice cybercriminals looking for effective ways to cause disruption online.

More details: [Sample screenshot of the actual advertisement:](#)

**Ganja**

DDoS for hire service advertisement showing various attack options and pricing.

**Hacking Alert**  
 Computer Tricks and Hacks. Hacking Software and much more ...

**#RefRef - The new DDoS Tool By Anonymous**  
 9:05 PM hacking 13 comments  
 Like 1.4k

**WE ARE ANONYMOUS**

Get Complete tutorial and Download link to #refref [HERE](#).

Novelty Signaling behavior is common... but analysts can't handle vast combinatorics with text-literal query interfaces

Options

Restricted Area [You are not protected] FBI / CIA / INTERPOL / NSA /

Allow command unknown attack  
 Hide data client monitoring  
 Hide data monitoring DHCP  
 Hide data client TCP/IP  
 Hide my IP  
 Don't DDoS me

Build Configuration

Port: 80 Threads: 100

Message TCP/UDP

**Go Go NSA Security**

Data Transmission Access:

ICMP Transmit Sent  IIS Transmit Sent  LOIC Transmit Sent  
 PHP Transmit Sent  ICP Transmit Sent  Torshammer Transmit Sent  
 Apache Transmit Sent  ISAT Transmit Sent  Slowloris Transmit Sent

Brute Attack:

TCP Socket Flood  HTTP Socket Flood  Automatic Socket Flood  
 TCP Packet Flood  HTTP Packet Flood  Automatic Packet Flood

The data on https requests for attack is impossible.

Execute Check Server Options Close

# Next Steps for Cyber and Crisis analysis SA

- On the ground now
  - Improve understanding of communication flows and community vocabularies within target domains to anticipate deliberate communication
  - Use current keyword based (e.g. ONRs TweetTracker) tools in a systematic manner to develop term use base-lines and to monitor for key tweets
- Future S&T
  - Develop next-generation analysis tools that ease burden on analysts and improve search results by leveraging social discourse structure

***Are you a hashtag? If I tweeted this, would it reach you?***

**Important workshop on social media impacts on human security & military operations. Be there. #nato #onr #dhs #red cross #UNHCR #GDACC #social media #humansecurity #cybersecurity #resiliency #disasterrelief #civilconflict #crisisoperations #privacy**



# SOARTECH

Modeling human reasoning.  
Enhancing human performance.