Explaining Cyber Crime Through the Lens of The Differential Association Theory

Rachel Levin
The College of New Jersey

Jonathan Richardson
Northern Kentucky University

Gary Warner & Dr. Kent Kerley
University of Alabama Birmingham

HADIDI44-2.PHP CASE STUDY

Thank you to the National Science Foundation' Research Experience for Undergraduates Program!


Sign Up | Log In | Help | Security Center
Search
PayPal
Change Your Language
U.S. English
Home
Personal
Business
Products & Services
Account login
Email address
Pay Pal password
New to Pay Pal? Sign up
Did you know?
How was this phish born?
Privacy | SSL Certificates | Legal Agreements | eBay
Copyright © 1999-2009 Pay Pal. All rights reserved.
Information about FDIC pass-through insurance

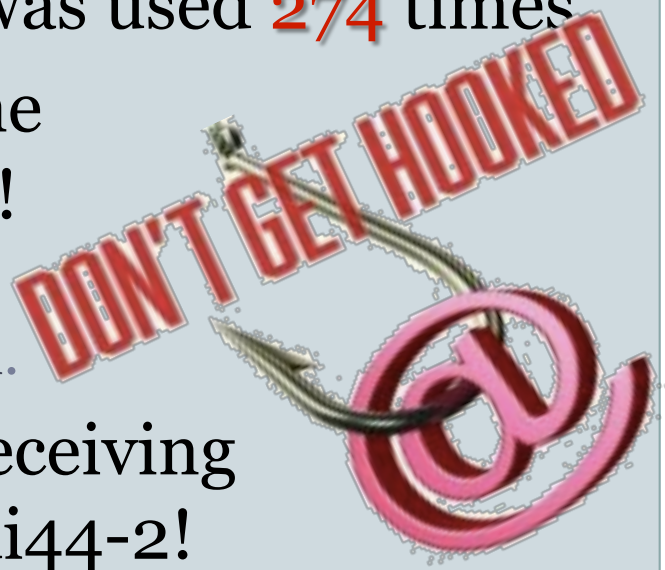
Phishing Kit

A ready to use file , usually in zip form, that contains all of the elements needed for a cyber-criminal or program to create a fictitious HTML website, more notably called a phish.

Case Study: *Hadidi44-2.php*

Why Hadidi44-2?

- Searched UAB Data Mine for unique phishing kits.
  - Many kits named login.php, update.php, etc..
- Came across the unique name hadidi44-2.php in one of our queries and used it to focus our search.
- The hadidi44-2.php phishing kit was used 274 times.
- There were 96 unique kits, with the only different being the action file!
  - An action file is a program that sends stolen credentials to the phisher's email.
- 99 unique email addresses were receiving stolen information through hadidi44-2!



What do we want to know?

Using Social Leaning Theory as a heuristic guide, we provide a case study on the phishing kit, hadidi44-2.php

- How was the hadidi44-2.php kit spread among so many criminals?
- Can this case study be explained through Edwin Sutherland's differential association theory?

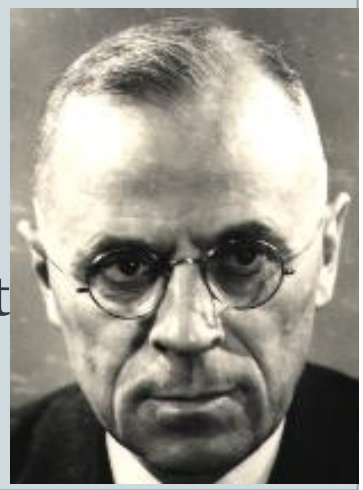
Possible Outcomes

3 POSSIBILITIES

1. The kit's creator had multiple email accounts and was spreading the kit from a plethora of different aliases
2. The kit was freely available on the Internet and any aspiring criminal could acquire and use it
3. The kit was distributed within a community of spammers who share their tools and techniques with one another

Differential Association Theory

- Short for "differential association with criminal and anti-criminal behavioral patterns."
- The content of learning is important
  - The process by which learning takes place is important
- The Basic Idea:
  - People learn deviant behavior through social interactions with criminal counterparts
  - Humans are a blank canvas. Criminals learn behaviors in the same way as non-offenders, except from a different group of people.
  - Does not explain who starts behavior or actions just how they are spread.



By associating with criminals one will learn the actions and skills of that person.

Differential Association Theory

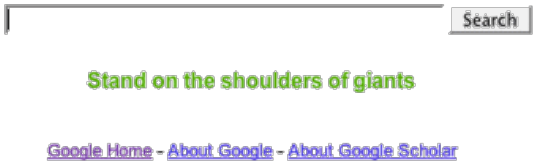
- Theory lies in nine propositions described by Mark M. Lanier and Stuart Henry:
  1. Criminal Behavior is learned
  2. Criminal behavior is learned in interaction with other persons in a process of communication.
  3. The principal part of the learning of criminal behavior occurs within intimate personal groups
  4. When criminal behavior is learned, the learning includes
     1. Techniques of committing the crime
     2. Specific direction of motives, drives rationalizations , and attitudes.

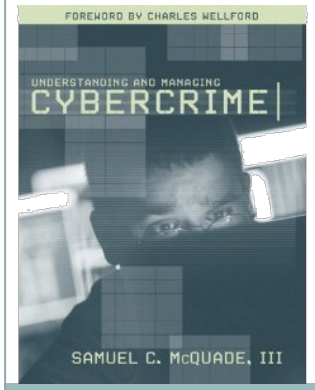
Differential Association Theory

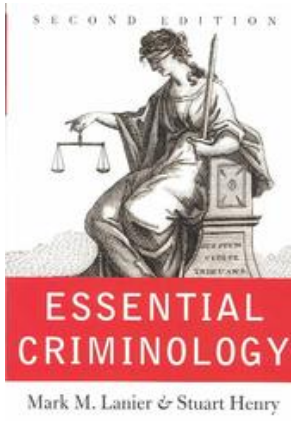
5. The specific direction of motives and drives is learned from definitions of legal codes as favorable and unfavorable.
6. A person becomes delinquent because of an excess of definitions favorable to violation of law over definitions unfavorable to violation of law.
7. Differential associations may vary in frequency, duration priority, and intensity.
8. Process of learning criminal behavior by association with the criminal and anti-criminal patterns involves all of the mechanisms that are involved in any other learning .
9. Though criminal behavior is an expression of general needs and values, it is not explained by those general needs and values since noncriminal behavior is an expression of the same needs and values (Sutherland 1947, 6-8).

- *The theory is usually used to explain street crime and white collar crime, but can it be applied to cyber crime?*

Research Tools



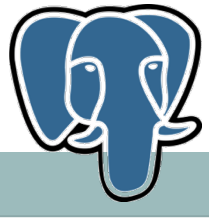




Methods of Research

STEPS OF RESEARCH

1. SQL Queries against UAB Phishing Data Mine
    1. Queries.
    2. Acquire list of target criminal emails.
2. Maltego
    1. Perform informed searches on known criminal email addresses from PostgreSQL.
    2. Gather search results, compile data for further research.
3. Google
    1. Search open source engine for clues.
    2. Utilize Google Translate.
4. Social Networking
    1. Search social networking sites for criminal aliases
5. I2 Analyst's Notebook
    1. Compile all information into a comprehensive link analysis c hart.



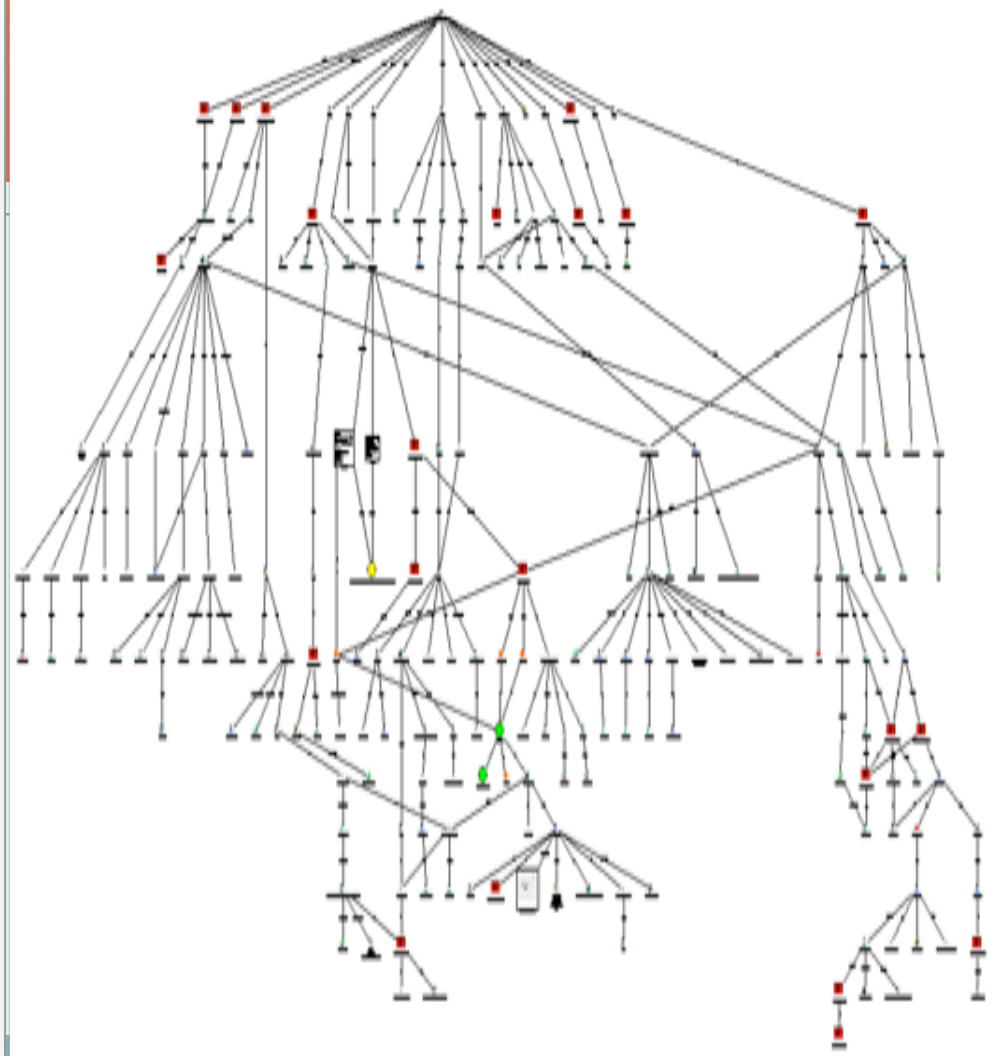

UAB Phishing Data Mine

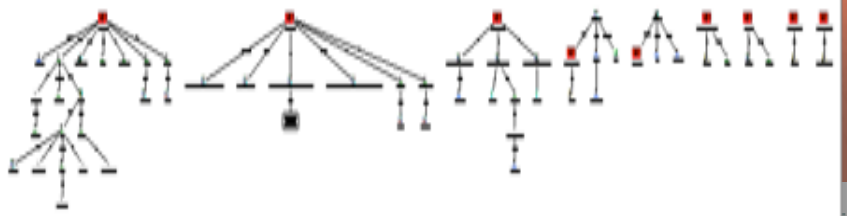
- As of July 18, 2012, the Phishing Ops team found 194,462 total recorded phish for this year.
- UAB retrieved phishing kits for 21,412 (11%) of the recorded phish.
- Refined parameters: Searched for keyword PayPal and found the hadidi44-2 kit
- Most active criminal used the kit 31 times.
- Different action files gave the kit a unique identifier called an MD5
  - There were 96 different MD5s because they all contained different "drop addresses"

Maltego

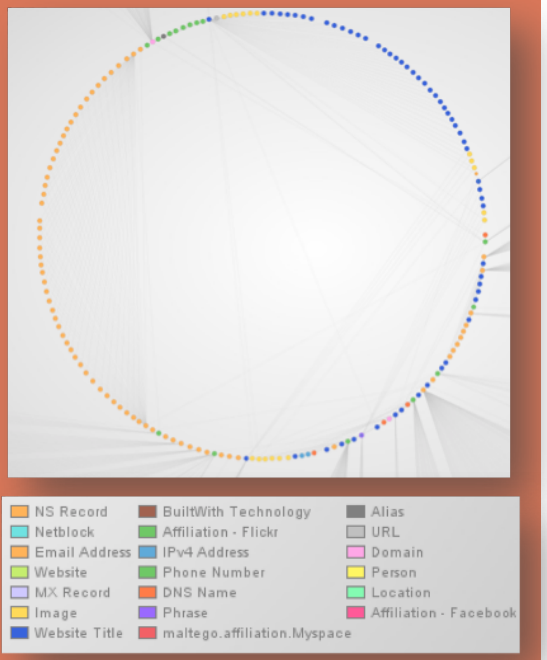
- ***Background*** – Open source intelligent source used to determine the relationships and real world links between
  - Aliases
  - Emails
  - Organizations
  - Websites
  - Computer Infrastructure
  - Contact Information
  - Phrases
  - Documents and Files
- Primary purpose – Lead Generation
  - Searched 99 emails using *Maltego* transformations

RESULTS





Maltego



Maltego results were refined when switching views.

- *Maltego*: provided clue generation
- Also returned a lot of unrelated results.
- For example, transformations were ran on the drop address, crywolef@yahoo.com, and yielded more than 50 results
  - Some results provided clues such as alter email addresses (crywole@yahoo.com) and registered websites (tahasocial.com, firemovies.net)
  - Other results not relevant (e.g cry_no_more@hotmail.com)

- The initial clues provided by *Maltego* were refined by additional searches in the *Google* search engine.
- Of the 99 unique emails behind the hadidi44-2.php phishing kit, 43 emails were found on the Internet
  - 32 emails returned ample and significant results not only on the criminals themselves, but also the way in which they were able to obtain hadidi44-2.
- Criminals showed an online presence on Arabic hacker forums.
  - Sa3eka, traidnt.net, VBhacker, VBspiders, and gazahacker.net

Forums were found to create most of the relationships within our criminal web

Social Networking

- 29 emails had Facebook profiles
  - 11 had strict privacy settings, but links are noted on a spreadsheet for law enforcement
  - The others are ***STUPID!***
  - ***Ex: mootez.saad@gmail.com***
- Other forms of social networking were not very prevalent.

Where's Waldo?

THANK YOU MOOTEZ SAAD! ☺

Mootez Saad is friends with a *Facebook* group of the name Tunisian-Hackers

This is their *Facebook* page.

These notes reveal proof that they steal from *PayPal*!

Emails: bsebai@ymail.com; smatrix1@live.fr; smatrix4spam@gmail.com; cc4smatrix@gmail.com

smatrix1@live.fr hacks websites for fun! YAY!

Oh wait, you registered a website?

Thanks for your contact information! Law enforcement will appreciate it !

Where else can I find this scam?

- The link hosted on *Facebook* is inactive now
- Simply searching the components of the program led to a phishing kit directory
  - Unfortunately, the directory has been taken down
- *The kit was created by Dr. Spam whose email is zakprokiller@gmail.com*
  - *Guess what? He's also a hacker.*
  - *He also was the criminal who used the kit 31 times! Shocker!*
- Hadidi44-2.php was also found on the *sa3eka* forum
- The kit was also found to be used in an *AlertPay* scam

count	md5
68	4ff7eee0a779eaa7d324122747803aa
27	3a18cffa453bd0995996b4266ec68d6
17	a1144604ec038e48e93a31b17866a76a
14	490cc13ec4a247bb9074d18dfaafe1df
11	66d3838653afc6c832e7177dee1a524a
11	6180bca61fe633a9bcce7a60c9cc4202
10	10f9f428d357c24882fd900ee4e3426
10	d85cf518656d142b82de533d565d3dd
9	3eea342cf6a249c3f8f582bcf51be941
8	92848d371433ce32d3ad0153493c2b46
7	74574baa92cda8ebdedde4e3326751c6
7	ad9b5837dfe3da665ea69bbdc5496bc5
7	1082e9b55518505a60f74b04b332c8bb
6	db3f594accb624566de0aa09d0f7cc06
6	5e6e97df315a29c5bf4044e86f498aa4
6	58d179c863b6a6a337004570fc3776b
6	6cf920eb4b73b880e652e1be205667fc
5	7ae6d1bc3e4a4bc7ebbdc95d0a91a1d8
5	d442f55eb7b96c612451e7f8c5560ef4
5	9c1892f191e9a91baf381442c78ac0b2
4	80662a0e6592cae66b6d277593cd35be
4	bffd0a0ea2ed28ad9e72a9bc127f77c
4	a6656c86d1b2afc8f581d84864bf027d
4	255b030071d087da32ee582f641ff37e
4	ddc3b3134346beb51cb792b517aa6595
4	aa6e17dfd27e911d29dd14bd3a5b4ae6
3	ed42211b6080f7a46a3e79d915c2af75
3	f6244e504afbe06f2ad97021e2b9eccc
3	7dded35f6aa183792a1b6030bdb75541
3	9df6af8a3e8da18f146e29ed560f84e
3	cebb1a9d435f4cdfe493fd6049048ca8
3	372923122fec7e2c5e1ed82a21699e5
3	7778cd775a0c60e94f6ccbecfb8b243b
3	8aef138a813bbbb7600837ce0f7a52b6

I2 Analyst Notebook

- Represents how the thirty-two most significant criminals relate to each other.
- The largest cluster contains 23 of the drop addresses associated with hadidi44-2.php.
  - This cluster also contains detailed information regarding relationships to the criminals to *Facebook* pages, aliases, alternate email addresses, and Arabic forum memberships.
- ***Click here to see the web of criminals!***

What was the outcome?

- Cyber criminals were found to share their tools freely in tight knit online communities.
- Although shared freely, our research shows that cyber criminals have formed intimate communities where they have developed a sense of trust and friendship.
  - In their cyber bubbles they are able to learn from each other by sharing ideas, practices, and tools of injustice.
  - Public upload into these close criminal communities allowed for different cyber criminals to associate with one another for a common purpose.
- ***The process of the spread of the hadidi44-2 kit can therefore be explained through differential association theory.***

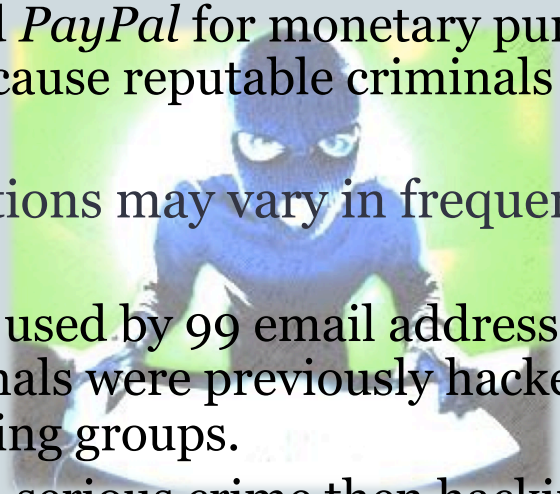
Explanations

- Which of the nine components of the differential association theory can be explained with this case study.
  1. Cyber criminal behavior was learned. We know this because usage of kit had grown exponentially.
  2. Cyber criminal behavior was learned in interaction with other criminals in a process of virtual communication through forums and social networking mediums.
     1. *Though physical proximity was not present, there was a close association in the virtual world.*
  3. The principal part of the learning of cyber criminal behavior occurred within intimate online criminal communities.

Explanations

4. When cyber criminal behavior was learned, the learning included
   - Techniques and skills of phishing (availability of the kit)
   - Specific direction of motives, drives, rationalizations, and attitudes. Criminals targeted *PayPal* for monetary purposes and believed it was acceptable because reputable criminals within the forums were spreading the kit.
7. Differential associations may vary in frequency, duration, priority, and intensity.
   - This kit was being used by 99 email addresses. However, most of these found criminals were previously hackers associated with their own smaller hacking groups.
   - Phishing is a more serious crime then hacking that involves much more involvement and instead of defacing websites, they are stealing money, identities, etc.

- *We do not know if the other components apply in this case because we do not know the full history of the criminals involved.*



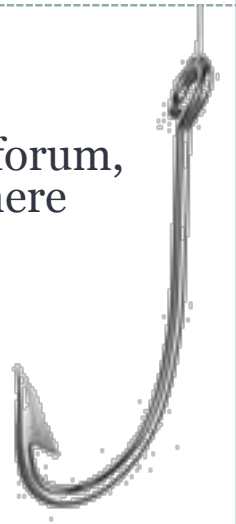
Problems

Problems surfaced while conduction this case study included:

1. Null Results
2. Finding the same alias for multiple people
3. Irrelevant Maltego results.
4. Language Barriers

Conclusion

- Our original problem:
  - How was the hadidi44-2.php kit spread among so many criminals?
    - Hadidi44-2 was found to be distributed on a close knit cyber criminal forum, and advertized through a link on a Facebook Tunisian-Hacker page where criminals formed a cyber community.
  - Can this case study be explained through Edwin Sutherland's differential association theory?
    - Cyber criminals associated with this phishing kit were able to learn deviant behavior through online interactions with criminal counterparts, propagating the hadidi44-2.php phishing kit.



Why does this matter?

- Future work can be done to relate more social theories to cyber crime.
- Doing so can help law enforcement understand of cyber crime through existing criminological theories.


KEEP
CALM
AND
REPORT
PHISHING
Copyright 2010 MindfulSecurity.com The Awareness Resource All Rights Reserved.