secure
sba-research.org

Ethics in Security Research

Which lines should not be crossed?

Sebastian Schrittwieser, Martin Mulazzani, Edgar Weippl

Spam Analytics: An Empirical Analysis of Spam Marketing Conversion

Christian Kreibich† Kirill Levchenko*
Geoffrey M. Voelker* Vern Paxson*†
International Computer Science Institute
Berkeley, USA
icir.org,vern@cs

Your Botnet is My Botnet: Analysis of a Botnet Takeover

Brett Stone-Gross, Ma
Richard Ke
Department
{bstone,marco

ABSTRACT

Botnets, networks of malware-infected
by an adversary, are the root cause of
problems on the Internet. A particula
ous type of bot is Torpig, a malware
harvest sensitive information (such as
data) from its victims. In this paper, w
control of the Torpig botnet and stud
ten days. During this time, we obse
infections and recorded almost 70

Is the Internet for Porn?
An Insight Into the Online Adult Industry

Christopher Kruegel[3]

PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs

Pitsillidis* Grant Jordan* Nicholas Weaver*† Christian
eoffrey M. Voelker* Stefan Savage* Kirill Levchenko*
Science *Department of Computer Science and
ty University of Californ
Computer Science Institute
rkeley, CA

Shining Light in Dark Places: Understanding the Tor Network

Damon McCoy
Tadayoshi
[1] Depa

@spam: The Underground on 140 Characters or Less *

Chris Grier† Kurt Thomas* Vern Paxson† Michael Zhang†
*University of Illinois, Champaign-Urbana
kathoma2@illinois.edu

Ideas of this talk

- Proposal of fundamental ethical principles
- Analysis of their role in recent papers
- Discussion - no judgement!

Ethical Principles

Do not harm humans actively!

Tuskegee syphilis experiment

- Patients were not informed about available treatments
- No precautions were taken that patients did not infect others
- They were also actively given false information regarding treatment


InfoSec research:
What could
possibly go wrong?

Scandal grows over fake Cra

news.cnet.com/8301-10784_3-6114909-7.html

2012 HOLIDAY GIFT GUIDE

Reviews | News | Download | CNET TV | How To | Deals

CNET › News › News Blogs › Scandal grows over fake Craigslist sex ad

Scandal grows over fake Craigslist sex ad

by Mike Yamamoto | September 12, 2006 12:55 PM PDT

0 0 0 +1 0 More + Comments 4

Girl wants to meet boy. Girl posts on Craigslist for a "casual encounter." Hundreds of boys respond.

This normally wouldn't be an unanticipated outcome, but what if the girl wasn't really a girl? And what if the imposter then took all the names, e-mail addresses and phone numbers sent by the men who responded and posted them all on the Web?

That's precisely what Jason Fortuny did in a "social experiment" that has generated a huge controversy, much of it in the form of a backlash that has included talk of litigation and even death threats. The Seattle Web developer has reportedly removed some of his own online information, which included his home address, phone number and photos (much of which is still available in archived versions of his various posts).

- Hoax ad on Craigslist
- Sexually explicit ad posted as a woman
- More than 100 men responded
- Their names, pictures, e-mail and phone numbers were published
- Possible results: divorces, firings, lawsuits, etc.

Do not watch bad things happening!

Spamalytics: An Empirical Analysis of Spam Marketing Conversion

Chris Kanich* Christian Kreibich† Kirill Levchenko* Brandon Enright*
Geoffrey M. Voelker* Vern Paxson† Stefan Savage*

†International Computer Science Institute
Berkeley, USA
christian@icir.org,vern@cs.berkeley.edu

*Dept. of Computer Science and Engineering
University of California, San Diego, USA
{ckanich,klevchen,voelker,savage}@cs.ucsd.edu
bmenrigh@ucsd.edu

ABSTRACT

The "conversion rate" of spam — the probability that an unsolicited e-mail will ultimately elicit a "sale" — underlies the entire spam value proposition. However, our understanding of this critical behavior is quite limited, and the literature lacks any quantitative study concerning its true value. In this paper we present a methodology for measuring the conversion rate of spam. Using a parasitic infiltration of an existing botnet's infrastructure, we analyze two spam campaigns: one designed to propagate a malware Trojan, the other marketing on-line pharmaceuticals. For nearly a half billion spam e-mails we identify the number that are successfully delivered, the number that pass through popular anti-spam filters, the number that elicit user visits to the advertised sites, and the number of "sales" and "infections" produced.

Categories and Subject Descriptors

K.4.1 [**Public Policy Issues**]: ABUSE AND CRIME INVOLVING COMPUTERS

General Terms

Measurement, Security, Economics

Keywords

Spam, Unsolicited Email, Conversion

Unraveling such questions is *essential* for understanding the economic support for spam and hence where any structural weaknesses may lie. Unfortunately, spammers do not file quarterly financial reports, and the underground nature of their activities makes third-party data gathering a challenge at best. Absent an empirical foundation, defenders are often left to speculate as to how successful spam campaigns are and to what degree they are profitable. For example, IBM's Joshua Corman was widely quoted as claiming that spam sent by the Storm worm alone was generating "millions and millions of dollars every day" [2]. While this claim could in fact be true, we are unaware of any public data or methodology capable of confirming or refuting it.

The key problem is our limited visibility into the three basic parameters of the spam value proposition: the cost to send spam, offset by the "conversion rate" (probability that an e-mail sent will ultimately yield a "sale"), and the marginal profit per sale. The first and last of these are self-contained and can at least be estimated based on the costs charged by third-party spam senders and through the pricing and gross margins offered by various Internet marketing "affiliate programs".[1] However, the conversion rate depends fundamentally on group actions — on what hundreds of millions of Internet users do when confronted with a new piece of spam — and is much harder to obtain. While a range of anecdotal numbers exist, we are unaware of any well-documented measurement of the spam conversion rate.[2]

In part, this problem is methodological. There are no apparent

- *"passive actors"*
  - Watching without helping
  - The researchs knew which computers were infected and simply watched without taking actions
- Analogy
  - Observing muggers at a backstreet without calling the police?

Spamalytics: An Empirical Analysis of Spam Marketing Conversion

- *"damage to victims [...] would be minimized"*
  - Victims were only informed after the experiments
  - Again: watching without helping

Your Botnet is My Botnet: Analysis of a Botnet Takeover

Do not perform illegal activities to harm illegal activities!

Your Botnet is My Botnet: Analysis of a Botnet Takeover

Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski,
Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna
Department of Computer Science, University of California, Santa Barbara
{bstone,marco,sullivan,rgilbert,msz,kemm,chris,vigna}@cs.ucsb.edu

ABSTRACT

Botnets, networks of malware-infected machines that are controlled by an adversary, are the root cause of a large number of security problems on the Internet. A particularly sophisticated and insidious type of bot is Torpig, a malware program that is designed to harvest sensitive information (such as bank account and credit card data) from its victims. In this paper, we report on our efforts to take control of the Torpig botnet and study its operations for a period of ten days. During this time, we observed more than 180 thousand infections and recorded almost 70 GB of data that the bots collected. While botnets have been "hijacked" and studied previously, the Torpig botnet exhibits certain properties that make the analysis of the data particularly interesting. First, it is possible (with reasonable accuracy) to identify unique bot infections and relate that number to the more than 1.2 million IP addresses that contacted our command and control server. Second, the Torpig botnet is large, targets a variety of applications, and gathers a rich and diverse set of data from the infected victims. This data provides a new understanding of the type and amount of personal information that is stolen by botnets.

Categories and Subject Descriptors

with a bot, the victim host will join a botnet, which is a network of compromised machines that are under the control of a malicious entity, typically referred to as the botmaster. Botnets are the primary means for cyber-criminals to carry out their nefarious tasks, such as sending spam mails [36], launching denial-of-service attacks [29], or stealing personal data such as mail accounts or bank credentials [16, 39]. This reflects the shift from an environment in which malware was developed for fun, to the current situation, where malware is spread for financial profit.

Given the importance of the problem, significant research effort has been invested to gain a better understanding of the botnet phenomenon.

One approach to study botnets is to perform *passive analysis* of secondary effects that are caused by the activity of compromised machines. For example, researchers have collected spam mails that were likely sent by bots [47]. Through this, they were able to make indirect observations about the sizes and activities of different spam botnets. Similar measurements focused on DNS queries [34, 35] or DNS blacklist queries [37] performed by bot-infected machines. Other researchers analyzed network traffic (netflow data) at the tier-1 ISP level for cues that are characteristic for certain botnets (such as scanning or long-lived IRC connections) [24]. While the analy-

- Intercepting a “legal botnet” (SETI@home) would be unethical

- Is a similar activity ethical simply because it is aimed at “bad” people?

- No argument of self-defense can be made!

Your Botnet is My Botnet: Analysis of a Botnet Takeover

- *"some [...] contents have already been widely and publicly documented. Consequently, we cannot create any new harm simply through association with these entities or repeating these findings"*

- Argument: everyone does it that way…

PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs

Do not conduct undercover research!

Is the Internet for Porn?
An Insight Into the Online Adult Industry

Gilbert Wondracek[1], Thorsten Holz[1], Christian Platzer[1],
Engin Kirda[2], and Christopher Kruegel[3]

[1]Secure Systems Lab,
Technical University Vienna

[2]Institute Eurecom,
Sophia Antipolis

[3]University of California,
Santa Barbara

Abstract

The online adult industry is among the most profitable business branches on the Internet, and its web sites attract large amounts of visitors and traffic. Nevertheless, no study has yet characterized the industry's economical and security-related structure. As cyber-criminals are motivated by financial incentives, a deeper understanding and identification of the economic actors and interdependencies in the online adult business is important for analyzing security-related aspects of this industry.

In this paper, we provide a survey of the different economic roles that adult web sites assume, and highlight their economic and technical features. We provide insights into security flaws and potential points of interest for cyber-criminals. We achieve this by applying a combination of automatic and manual analysis techniques to investigate the economic structure of the online adult industry and its business cases. Furthermore, we also performed several experiments to gain a better understanding of the flow of visitors

Apparently, even roughly estimating the size of the Internet porn industry is non-trivial, as different sources [2, 10, 28] indicate a yearly total revenue that ranges from 1 to 97 billion USD. Yet, even the lowest of these estimates hints at the economic significance of this market.

Interestingly, however, to the best of our knowledge, no study has yet been published that analyzes the economical and technological structure of this industry from a security point of view. In this work, we aim at answering the following questions:

Which economic roles exist in the online adult industry? Our analysis shows that there is a broad array of economic roles that web sites in this industry can assume. Apart from the purpose of selling pornographic media over the Internet, there are much less obvious and visible business models in this industry, such as *traffic trading* web sites or *cliques* of business competitors who cooperate to increase their revenue. We identify, in this paper, the main economic roles of the adult industry and show the associated revenue models, organizational structures, technical features and interdepen-

- *"we believe that realistic experiments are the only way to reliably estimate success rates of attacks in the real-world"*

- We had to do it that way...

- Does not solve the ethical dilemma!

Is the Internet for Porn?
An Insight Into the Online Adult Industry

Conclusions

- InfoSec research community is well aware of ethical questions within their field
- However, even the most fundamental ethical principles are difficult to fulfill
- Things are changing fast in information technology. Threat of guidelines that do not reflect the actual technological environment?

Thank you for your attention!

sschrittwieser@sba-research.org