Beyond Technical Security: Developing an Empirical Basis for Socio-Economic Perspectives

Vern Paxson

International Computer Science Institute
EECS Department, University of California
Berkeley, California USA
vern@icsi.berkeley.edu

October 12, 2012

THE DAILY CALIFORNIAN | NEWS

RESEARCH & IDEAS

FRIDAY, SEPTEMBER 28, 2012

Cybercrime project receives $10 million from NSF

BY CAROLINE MURPHY | STAFF

A project conducted by researchers from the UC Berkeley-affiliated International Computer Science Institute, UC San Diego and George Mason University has received a $10 million, five-year grant from the National Science Foundation to study social and economic issues connected to cybercrime.

While much of cyber-security research focuses on the technological side of attacks, Beyond Technical Security: Developing an Empirical Basis for Socio-Economic Perspectives will take an interdisciplinary look into cybercriminals — how they work with each other, the marketplaces that they work in and the profit they gain.

TWC: Frontier: Collaborative:
Beyond Technical Security: Developing an Empirical Basis for Socio-Economic Perspectives

Stefan Savage, Geoffrey M. Voelker, James Fowler, Alex Snoeren,
Lawrence Saul, Kirill Levchenko, Erin Kenneally
University of California, San Diego

Vern Paxson, Mark Allman, Chris Grier, Chris Hoofnagle, Dan Klein,
Christian Kreibich, Deirdre Mulligan, Nicholas Weaver
International Computer Sciences Institute

Damon McCoy
George Mason University

September 2012 – August 2017

TWC: Frontier: Collaborative:
Beyond Technical Security: Developing an Empirical Basis for Socio-Economic Perspectives

Stefan Savage, Geoffrey M. Voelker, James Fowler, Alex Snoeren,
Lawrence Saul, Kirill Levchenko, Erin Kenneally
University of California, San Diego

Vern Paxson, Mark Allman, Chris Grier, Chris Hoofnagle, Dan Klein,
Christian Kreibich, Deirdre Mulligan, Nicholas Weaver
International Computer Sciences Institute

Damon McCoy
George Mason University

September 2012 – August 2017

A Proposal to DARPA in Response to

BAA03-18

DYNAMIC QUARANTINE OF COMPUTER WORM-BASED ATTACKS AGAINST MILITARY ENTERPRISE NETWORKS

Lead Organization	Silicon Defense
Type of Business	Other Small Business
Other Team Members	The International Computer Science Institute (ICSI) Other Non-Profit
	University of California, San Diego Other Educational
	The Boeing Company Large Business
	Lawrence Berkeley National Laboratory Other Non-Profit
Proposal Title	Defense of Military Networks against Worms

A Proposal to DARPA in Response to

BAA03-18

DYNAMIC QUARANTINE OF COMPUTER WORM-BASED ATTACKS AGAINST MILITARY ENTERPRISE NETWORKS

Revised in light of Draft Security Classification Guide

Lead Organization	Silicon Defense
Type of Business	Other Small Business
Other Team Members	The International Computer Science Institute (ICSI) Other Non-Profit
	University of California, San Diego Other Educational
	The Boeing Company Large Business
	Lawrence Berkeley National Laboratory Other Non-Profit
Proposal Title	Defense of Military Networks against Worms

NSF CyberTrust Center Proposal

Center for Internet Epidemiology and Defenses

Stefan Savage, Geoffrey M. Voelker, George Varghese
University of California, San Diego

Vern Paxson, Nicholas Weaver
International Computer Sciences Insitute

October 2004–September 2009

CCIED Collaborative Center for Internet Epidemiology and Defenses

A UCSD and ICSI Joint NSF Cyber Trust Center

2005

Case Study: A Failure Wrapped in Success' Clothing - On the Need for Sound Forensics in Handling Digital Evidence Cases, Erin E. Kenneally and Andrea Monti, Digital Investigation, Elsevier Ltd., Winter 2005.

Using Honeynets for Internet Situational Awareness, Vinod Yegneswaran, Paul Barford, and Vern Paxson, Proceedings of the 4th ACM Workshop on Hot Topics in Networks (HotNets-IV), College Park, MD, November 2005.

Opportunistic Measurement: Extracting Insight from Spurious Traffic, Martin Casado, Tal Garfinkel, Weidong Cui, Vern Paxson, and Stefan Savage, Proceedings of the 4th ACM Workshop on Hot Topics in Networks (HotNets-IV), College Park, MD, November 2005.

Self-stopping Worms, Justin Ma, Geoffrey M. Voelker, and Stefan Savage, Proceedings of the ACM Workshop on Rapid Malcode (WORM), Washington D.C., November 2005.

Scalability, Fidelity and Containment in the Potemkin Virtual Honeyfarm, Michael Vrable, Justin Ma, Jay Chen, David Moore, Erik VandeKieft, Alex C. Snoeren, Geoffrey M. Voelker, and Stefan Savage, Proceedings of the 20th ACM Symposium on Operating System Principles (SOSP), Brighton, UK, October 2005.

Exploiting Underlying Structure for Detailed Reconstruction of an Internet-scale Event, Abhishek Kumar, Vern Paxson, and Nicholas Weaver, Proceedings of the USENIX/ACM Internet Measurement Conference, New Orleans, LA, October 2005.

Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection, Erin E. Kenneally, UCLA Journal of Law and Technology, 2005.

2004

Automated Worm Fingerprinting, Sumeet Singh, Cristian Estan, George Varghese, and Stefan Savage, Proceedings of the 6th ACM/USENIX Symposium on Operating System Design and Implementation (OSDI), San Francisco, CA, December 2004.

On the Difficulty of Scalably Detecting Network Attacks, Kirill Levchenko, Ramamohan Paturi, and George Varghese, Proceedings of the ACM Conference on Computer and Communications Security, Washington, D.C., October 2004.

Preliminary Results Using ScaleDown to Explore Worm Dynamics, Nicholas Weaver, Ihab Hamadeh, George Kesidis, and Vern Paxson, Proceedings of the ACM Workshop on Rapid Malcode (WORM), Washington, D.C., October 2004.

The Top Speed of Flash Worms, Stuart Staniford, David Moore, Vern Paxson, and Nicholas Weaver, Proceedings of the ACM Workshop on Rapid Malcode (WORM), Washington, D.C., October 2004.

On Scalable Attack Detection in the Network, Ramana Rao Kompella, Sumeet Singh, and George Varghese, Proceedings of the USENIX/ACM Internet Measurement Conference, Taormina, Sicily, Italy, October 2004.

FINAL PROGRAM

2006 IEEE Symposium on Security and Privacy

May 21-24, 2006

The Claremont Resort
Berkeley/Oakland, California, USA

Monday, May 22, 2006

8:45-9:00	**Opening Remarks** (Hilarie Orman, Vern Paxson)
9:00-10:30	**Session: Signature Generation** (Christopher Kruegel) *Towards Automatic Generation of Vulnerability-Based Signatures* David Brumley, James Newsome, Dawn Song, Hao Wang, and Somesh Jha Carnegie Mellon University, USA, and University of Wisconsin, USA (30 minutes) *Misleading Worm Signature Generators Using Deliberate Noise Injection* Roberto Perdisci, David Dagon, Wenke Lee, Prahlad Fogla, and Monirul Sharif University of Cagliari, Italy, and Georgia Institute of Technology, USA (30 minutes) *Hamsa: Fast Signature Generation for Zero-day Polymorphic Worms with Provable Attack Resilience* Zhichun Li, Manan Sanghi, Yan Chen, Ming-Yang Kao and Brian Chavez Northwestern University, USA (30 minutes)

TWC: Frontier: Collaborative: Beyond Technical Security: Developing an Empirical Basis for Socio-Economic Perspectives

Stefan Savage, Geoffrey M. Voelker, James Fowler, Alex Snoeren,
Lawrence Saul, Kirill Levchenko, Erin Kenneally
University of California, San Diego

Vern Paxson, Mark Allman, Chris Grier, Chris Hoofnagle, Dan Klein,
Christian Kreibich, Deirdre Mulligan, Nicholas Weaver
International Computer Sciences Institute

Damon McCoy
George Mason University

September 2012 – August 2017

CCIED Collaborative Center for Internet Epidemiology and Defenses

A UCSD and ICSI Joint NSF Cyber Trust Center

2007

Can You Infect Me Now? Malware Propagation in Mobile Phone Networks, Chris Fleizach, Michael Lilijenstam, Per Johansson, Geoffrey M. Voelker, and András Méhes, Proceedings of the ACM Workshop on Recurring Malcode (WORM), Washington D.C., November 2007.

Issues and Etiquette Concerning Use of Shared Measurement Data, Mark Allman and Vern Paxson, Proceedings of the ACM Internet Measurement Conference, San Diego, CA, October 2007.

A Brief History of Scanning, Mark Allman, Vern Paxson, and Jeff Terrell, Proceedings of the ACM Internet Measurement Conference, San Diego, CA, October 2007.

Shunting: A Hardware/Software Architecture for Flexible, High-Performance Network Intrusion Prevention, Jose Maria Gonzalez, Nicholas Weaver, and Vern Paxson, Proceedings of the ACM Conference on Computer and Communications Security, Alexandria, VA, October 2007.

An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants, Jason Franklin, Vern Paxson, Adrian Perrig, and Stefan Savage, Proceedings of the ACM Conference on Computer and Communications Security, Alexandria, VA, October 2007.

Spamscatter: Characterizing Internet Scam Hosting Infrastructure, David S. Anderson, Chris Fleizach, Stefan Savage, and Geoffrey M. Voelker, Proceedings of the USENIX Security Symposium, Boston, MA, August 2007.

Slicing Spam with Occam's Razor, Chris Fleizach, Geoffrey M. Voelker, and Stefan Savage, Proceedings of the Conference on Email and Anti-Spam (CEAS), Mountain View, CA, August 2007.

On the Adaptive Real-Time Detection of Fast-Propagating Network Worms, Jaeyeon Jung, Rodolfo A. Milito, and Vern Paxson, Proceedings of the Fourth GI International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment, Lucerne, Switzerland, July 2007.

The Shunt: An FPGA-Based Accelerator for Network Intrusion Prevention, Nicholas Weaver, Vern Paxson, and Jose M. Gonzalez, Proceedings of the ACM/SIGDA 15th International Symposium on Field Programmable Gate Arrays, February 2007.

2006

Glavlit: Preventing Exfiltration at Wire Speed, Nabil Schear, Carmelo Kintana, Qing Zhang, and Amin Vahdat, Proceedings of the 5th ACM Workshop on Hot Topics in Networks (HotNets-V), Irvine, CA, November 2006.

Fighting Coordinated Attackers with Cross-Organizational Information Sharing, Mark Allman, Ethan Blanton, Vern Paxson, and Scott Shenker, Proceedings of the 5th ACM Workshop on Hot Topics in Networks (HotNets-V), Irvine, CA, November 2006.

On the Adaptive Real-Time Detection of Fast-Propagating Network Worms, Jaeyeon Jung, Rodolfo A. Milito, and Vern Paxson, MIT technical report MIT-CSAIL-TR-2006-074, November 2006.

CCIED Collaborative Center for Internet Epidemiology and Defenses

A UCSD and ICSI Joint NSF Cyber Trust Center

2007

Can You Infect Me Now? Malware Propagation in Mobile Phone Networks, Chris Fleizach, Michael Lilijenstam, Per Johansson, Geoffrey M. Voelker, and András Méhes, Proceedings of the ACM Workshop on Recurring Malcode (WORM), Washington D.C., November 2007.

Issues and Etiquette Concerning Use of Shared Measurement Data, Mark Allman and Vern Paxson, Proceedings of the ACM Internet Measurement Conference, San Diego, CA, October 2007.

A Brief History of Scanning, Mark Allman, Vern Paxson, and Jeff Terrell, Proceedings of the ACM Internet Measurement Conference, San Diego, CA, October 2007.

Shunting: A Hardware/Software Architecture for Flexible, High-Performance Network Intrusion Prevention, Jose Maria Gonzalez, Nicholas Weaver, and Vern Paxson, Proceedings of the ACM Conference on Computer and Communications Security, Alexandria, VA, October 2007.

An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants, Jason Franklin, Vern Paxson, Adrian Perrig, and Stefan Savage, Proceedings of the ACM Conference on Computer and Communications Security, Alexandria, VA, October 2007.

Spamscatter: Characterizing Internet Scam Hosting Infrastructure, David S. Anderson, Chris Fleizach, Stefan Savage, and Geoffrey M. Voelker, Proceedings of the USENIX Security Symposium, Boston, MA, August 2007.

Slicing Spam with Occam's Razor, Chris Fleizach, Geoffrey M. Voelker, and Stefan Savage, Proceedings of the Conference on Email and Anti-Spam (CEAS), Mountain View, CA, August 2007.

On the Adaptive Real-Time Detection of Fast-Propagating Network Worms, Jaeyeon Jung, Rodolfo A. Milito, and Vern Paxson, Proceedings of the Fourth GI International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment, Lucerne, Switzerland, July 2007.

The Shunt: An FPGA-Based Accelerator for Network Intrusion Prevention, Nicholas Weaver, Vern Paxson, and Jose M. Gonzalez, Proceedings of the ACM/SIGDA 15th International Symposium on Field Programmable Gate Arrays, February 2007.

2006

Glavlit: Preventing Exfiltration at Wire Speed, Nabil Schear, Carmelo Kintana, Qing Zhang, and Amin Vahdat, Proceedings of the 5th ACM Workshop on Hot Topics in Networks (HotNets-V), Irvine, CA, November 2006.

Fighting Coordinated Attackers with Cross-Organizational Information Sharing, Mark Allman, Ethan Blanton, Vern Paxson, and Scott Shenker, Proceedings of the 5th ACM Workshop on Hot Topics in Networks (HotNets-V), Irvine, CA, November 2006.

On the Adaptive Real-Time Detection of Fast-Propagating Network Worms, Jaeyeon Jung, Rodolfo A. Milito, and Vern Paxson, MIT technical report MIT-CSAIL-TR-2006-074, November 2006.

CCIED Collaborative Center for Internet Epidemiology and Defenses

A UCSD and ICSI Joint NSF Cyber Trust Center

2007

Can You Infect Me Now? Malware Propagation in Mobile Phone Networks, Chris Fleizach, Michael Lilijenstam, Per Johansson, Geoffrey M. Voelker, and András Méhes, Proceedings of the ACM Workshop on Recurring Malcode (WORM), Washington D.C., November 2007.

Issues and Etiquette Concerning Use of Shared Measurement Data, Mark Allman and Vern Paxson, Proceedings of the ACM Internet Measurement Conference, San Diego, CA, October 2007.

A Brief History of Scanning, Mark Allman, Vern Paxson, and Jeff Terrell, Proceedings of the ACM Internet Measurement Conference, San Diego, CA, October 2007.

Shunting: A Hardware/Software Architecture for Flexible, High-Performance Network Intrusion Prevention, Jose Maria Gonzalez, Nicholas Weaver, and Vern Paxson, Proceedings of the ACM Conference on Computer and Communications Security, Alexandria, VA, October 2007.

An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants, Jason Franklin, Vern Paxson, Adrian Perrig, and Stefan Savage, Proceedings of the ACM Conference on Computer and Communications Security, Alexandria, VA, October 2007.

Spamscatter: Characterizing Internet Scam Hosting Infrastructure, David S. Anderson, Chris Fleizach, Stefan Savage, and Geoffrey M. Voelker, Proceedings of the USENIX Security Symposium, Boston, MA, August 2007.

Slicing Spam with Occam's Razor, Chris Fleizach, Geoffrey M. Voelker, and Stefan Savage, Proceedings of the Conference on Email and Anti-Spam (CEAS), Mountain View, CA, August 2007.

On the Adaptive Real-Time Detection of Fast-Propagating Network Worms, Jaeyeon Jung, Rodolfo A. Milito, and Vern Paxson, Proceedings of the Fourth GI International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment, Lucerne, Switzerland, July 2007.

The Shunt: An FPGA-Based Accelerator for Network Intrusion Prevention, Nicholas Weaver, Vern Paxson, and Jose M. Gonzalez, Proceedings of the ACM/SIGDA 15th International Symposium on Field Programmable Gate Arrays, February 2007.

2006

Glavlit: Preventing Exfiltration at Wire Speed, Nabil Schear, Carmelo Kintana, Qing Zhang, and Amin Vahdat, Proceedings of the 5th ACM Workshop on Hot Topics in Networks (HotNets-V), Irvine, CA, November 2006.

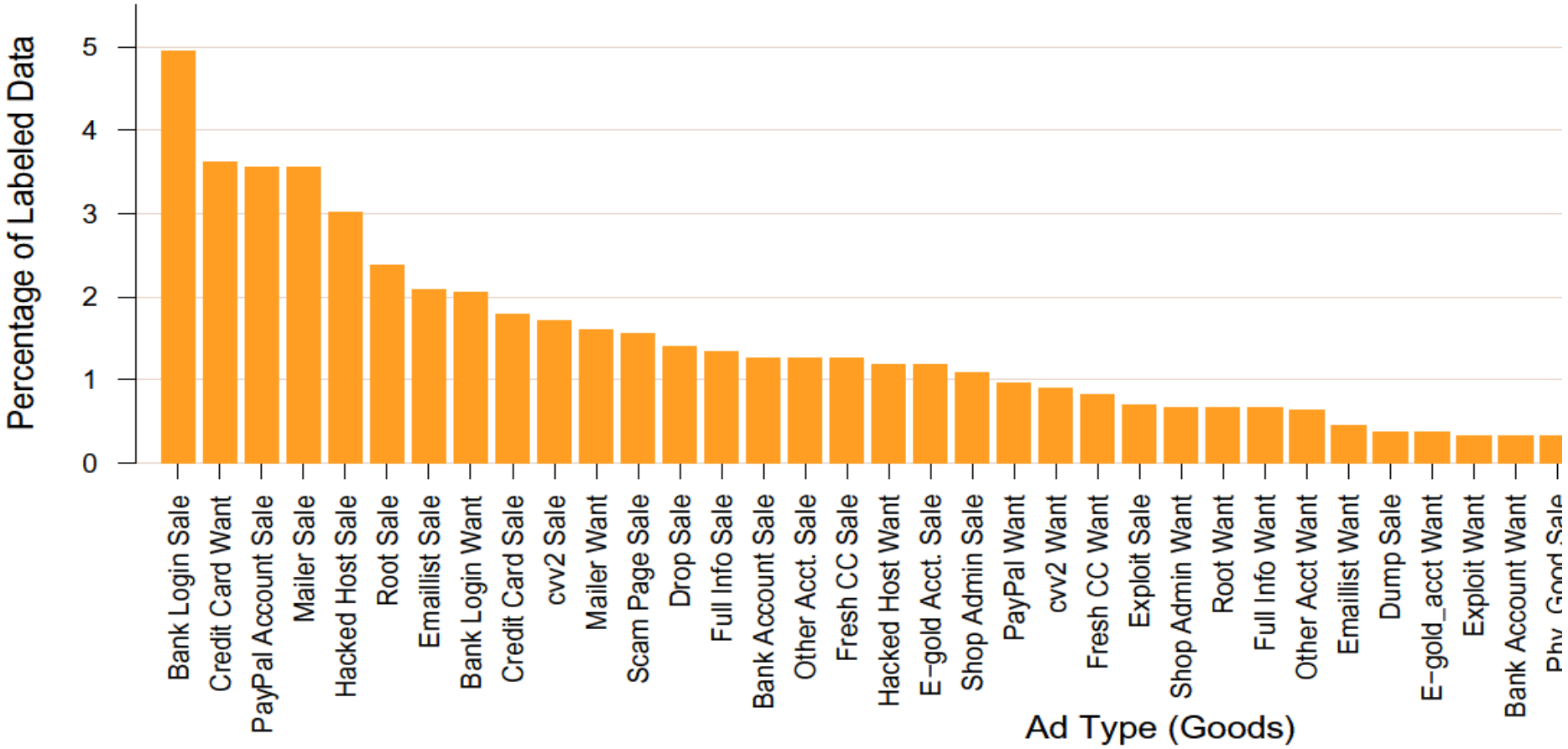
Fighting Coordinated Attackers with Cross-Organizational Information Sharing, Mark Allman, Ethan Blanton, Vern Paxson, and Scott Shenker, Proceedings of the 5th ACM Workshop on Hot Topics in Networks (HotNets-V), Irvine, CA, November 2006.

On the Adaptive Real-Time Detection of Fast-Propagating Network Worms, Jaeyeon Jung, Rodolfo A. Milito, and Vern Paxson, MIT technical report MIT-CSAIL-TR-2006-074, November 2006.

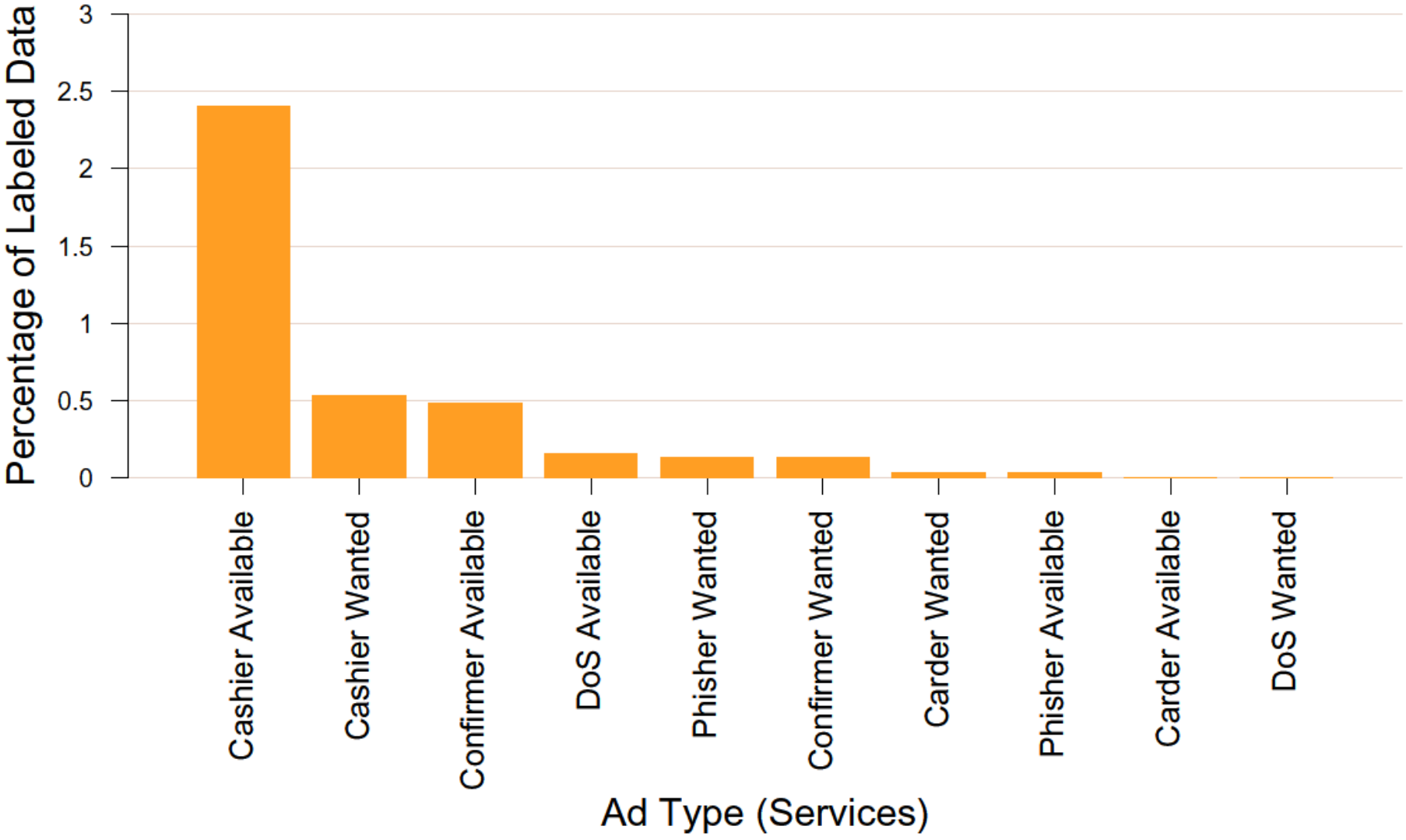
Advertisement

i have boa wells and barclays bank logins....
have hacked hosts, mail lists, php mailer send to all inbox
i need 1 mastercard i give 1 linux hacked root
i have verified paypal accounts with good balance...and i can cashout paypals

Marketplace Ads for Goods



Marketplace Ads for Services



Proposal Submitted to ONR BAA 08-019

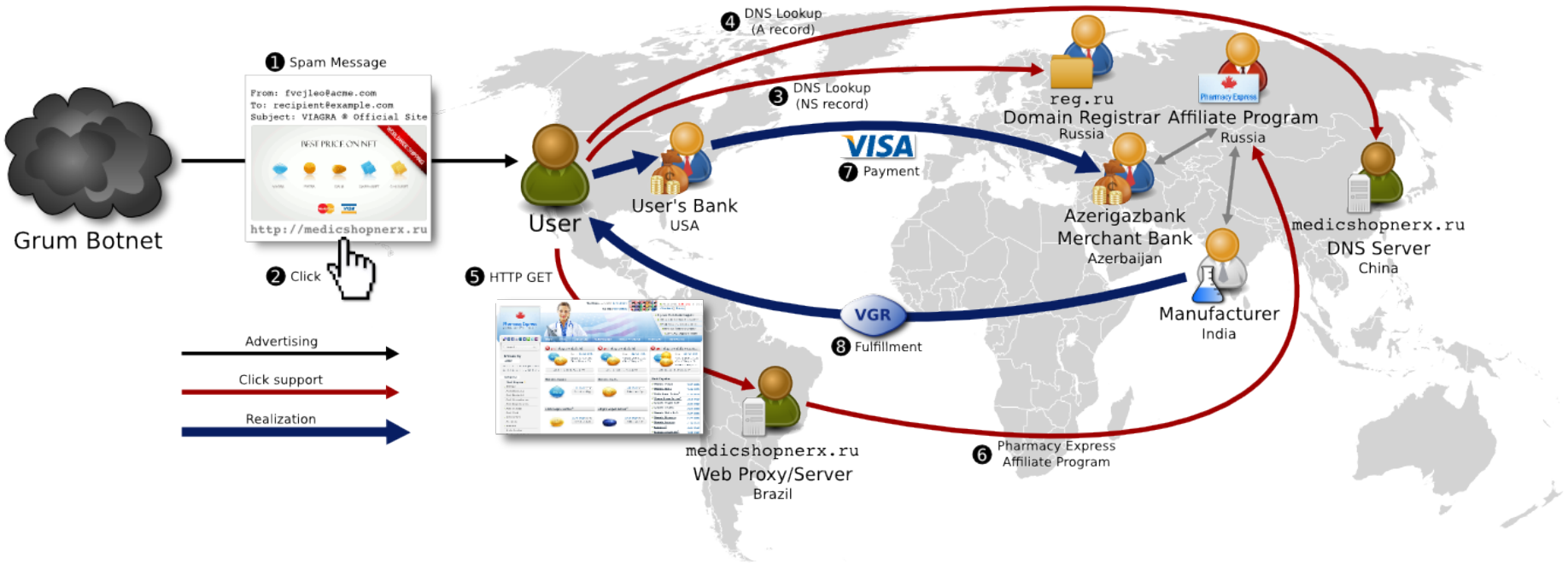
Proposal title:

Infiltration of Botnet Command-&-Control and Support Ecosystems

Principal Investigator	Stefan Savage Phone: 858-822-4895 Fax: 858-534-7029 Email: savage@cs.ucsd.edu
Institution	University of California, San Diego
Department	Computer Science & Engineering
Division	General Campus
Address	9500 Gilman Dr., Dept 0404 La Jolla, CA 92093-0404
Other Universities	University of California, Berkeley

Institution Proposal No.	2009-1976
Agency	ONR
Topic Number and Title	#2 — Removing the Botnet Threat

Phases of the Spam Value Chain



If we were to "snip" a link in this chain, which one would be the most disruptive for our least expenditure?

Proc. IEEE Security & Privacy 2011

Feed Name	*Feed Description*	*Received URLs*	*Distinct Domains*
Feed A	MX honeypot	32,548,304	100,631
Feed B	Seeded honey accounts	73,614,895	35,506
Feed C	MX honeypot	451,603,575	1,315,292
Feed D	Seeded honey accounts	30,991,248	79,040
Feed X	MX honeypot	198,871,030	2,127,164
Feed Y	Human identified	10,733,231	1,051,211
Feed Z	MX honeypot	12,517,244	67,856
Cutwail	Bot	3,267,575	65
Grum	Bot	11,920,449	348
MegaD	Bot	1,221,253	4
Rustock	Bot	141,621,731	13,612,815
Other bots	Bot	7,768	4
Total		968,918,303	17,813,952

Table I: Feeds of spam-advertised URLs used in this study. We collected feed data from August 1, 2010 through October 31, 2010.

Affiliate Program	URLs	Volume	Domains
RX–Promotion	160,522,026	21.7%	10,586
Mailien	69,961,211	23.57%	14,444
Pharmacy Express	69,959,633	23.57%	14,381
ED Express	1,578	<0.01%	63
ZedCash (Pharma)	42,297,130	18.93%	6,981
Dr. Maxman	32,184,860	13.19%	5,641
Viagrow	5,222,658	3.57%	386
US HealthCare Inc.	3,196,538	1.42%	167
MaxGentleman	1,144,703	0.39%	672
VigREX	426,873	0.31%	39
Stud Extreme	71,104	0.05%	43
ManXtenz	50,394	<0.01%	33
GlavMed	28,313,136	7.84%	2,933
Online Pharmacy	17,266,034	5.07%	2,922
EvaPharmacy	12,798,999	7.91%	11,285
World Pharmacy	10,412,850	5.88%	691
PH Online	2,971,368	2.14%	101
Swiss Apotheke	1,593,532	0.21%	118
HerbalGrowth	265,131	0.19%	17
RX Partners	229,248	0.15%	448
Stimul-cash	157,537	0.07%	50
MAXX Extend	104,201	<0.01%	23
DrugRevenue	51,637	0.05%	122
Ultimate Pharmacy	44,126	0.02%	12
Greenline	25,021	<0.01%	1,766
Virility	23,528	0.01%	9
MediTrust	6,156	<0.01%	24
RX Rev Share	5,690	<0.01%	183
Unknown Program	3,310	<0.01%	1,270
Canadian Pharmacy	1,392	<0.01%	133
RXCash	287	<0.01%	22
Stallion	80	<0.01%	2
Pharma Total	347,053,630	93.74%	54,142

Affiliate Program	URLs	Volume	Domains
Royal Software	2,291,571	1.48%	572
EuroSoft	694,810	0.31%	1,161
Auth. Soft. Resellers	65,918	<0.01%	4,117
OEM Soft Store	19,436	<0.01%	1,367
Soft Sales	93	<0.01%	35
Software Total	3,071,828	1.79%	7,252

Looked at three categories:
Pharma, Replica, Software

Covered all the major affiliate programs

Affiliate Program	URLs	Volume	Domains
ZedCash (Replica)	13,264,108	4.29%	7,011
Ultimate Replica	10,464,930	3.35%	5,032
Distinction Replica	1,252,816	0.3%	130
Diamond Replicas	506,486	0.14%	1,307
Prestige Replicas	382,964	0.16%	101
Exquisite Replicas	620,642	0.32%	128
One Replica	21,318	0.02%	83
Luxury Replica	11,207	<0.01%	28
Aff. Accessories	3,669	<0.01%	187
Swiss Rep. & Co.	76	<0.01%	15
WatchShop	2,086,930	0.17%	547
Replica Total	15,351,038	4.46%	7,558

PAIN RELIEF
- Vicodin ES
- Hydrocodone
- Percocet
- Lortab
- Darvocet (Proxyvon)
- Codeine
- **View all products**

ANTI-ANXIETY
- Xanax
- Valium (® ROCHE)
- Ativan (® Wyeth)
- Klonopin (generic)
- Valium (generic)
- Anti-Anxiety Pack
- Atarax
- **View all products**

ADHD Treatment
- Adderall
- Brand Ritalin
- **View all products**

WEIGHT LOSS
- Phentermine

Order approved

Your transaction has been approved.

Your order ID: 138730
First name: Geoff
Last name: Voelker
Card used with this order: 46*****2205
Total amount charged: $64.95

The following billing descriptor appear on your credit card statement:

==========

medissue.com +12175686119

==========

Tracking number will be sent on your email once medications will be shipped.

NOTE: Contact us about your order only through customers support system www.rxsup24.com
Before contact us and ask about time for delivery please read our shipping policy.

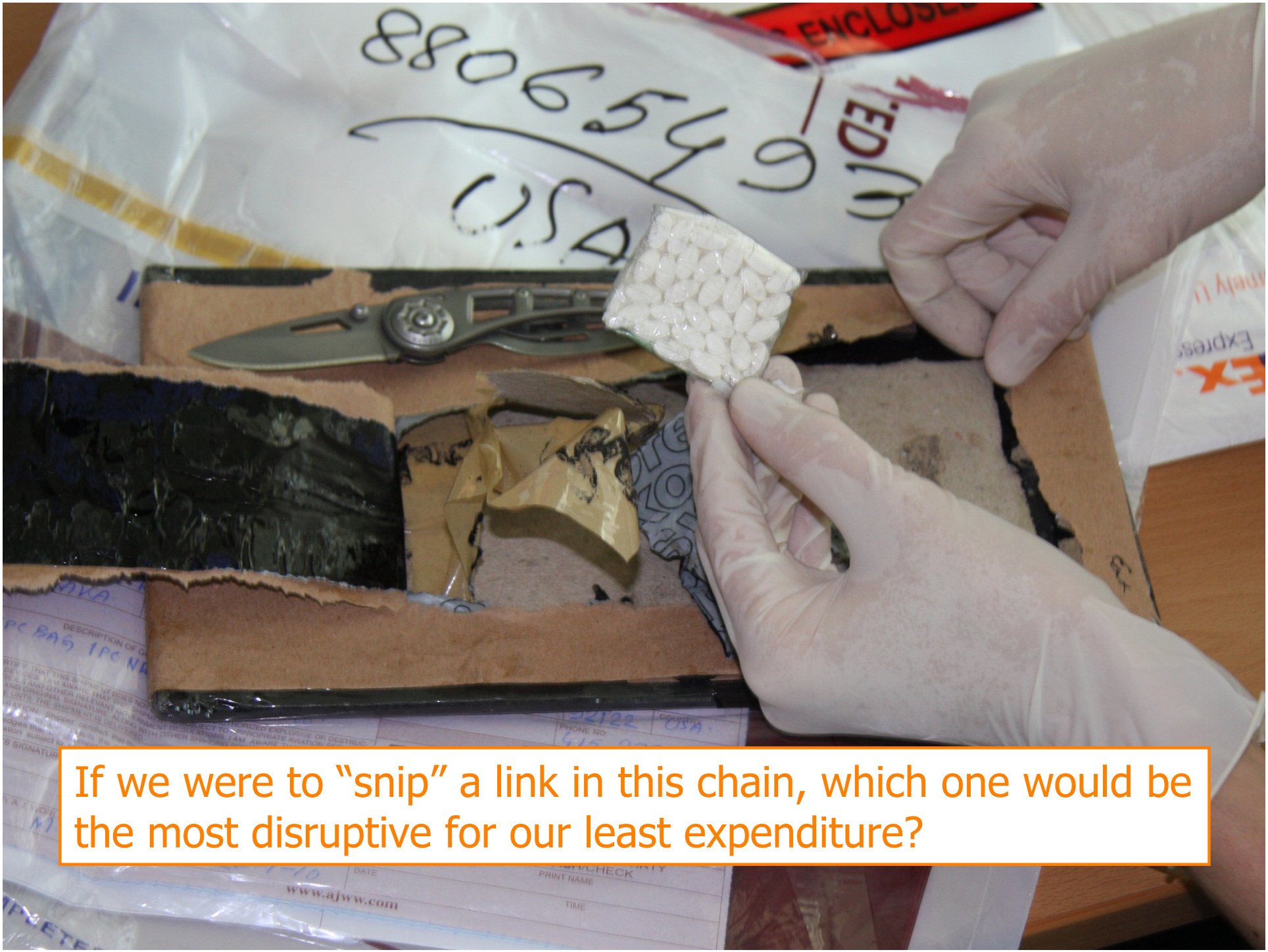
ORDER STATUS, TRACKING NUMBER, FAQ ABOUT DELIVERY:

Website menu --> Order status

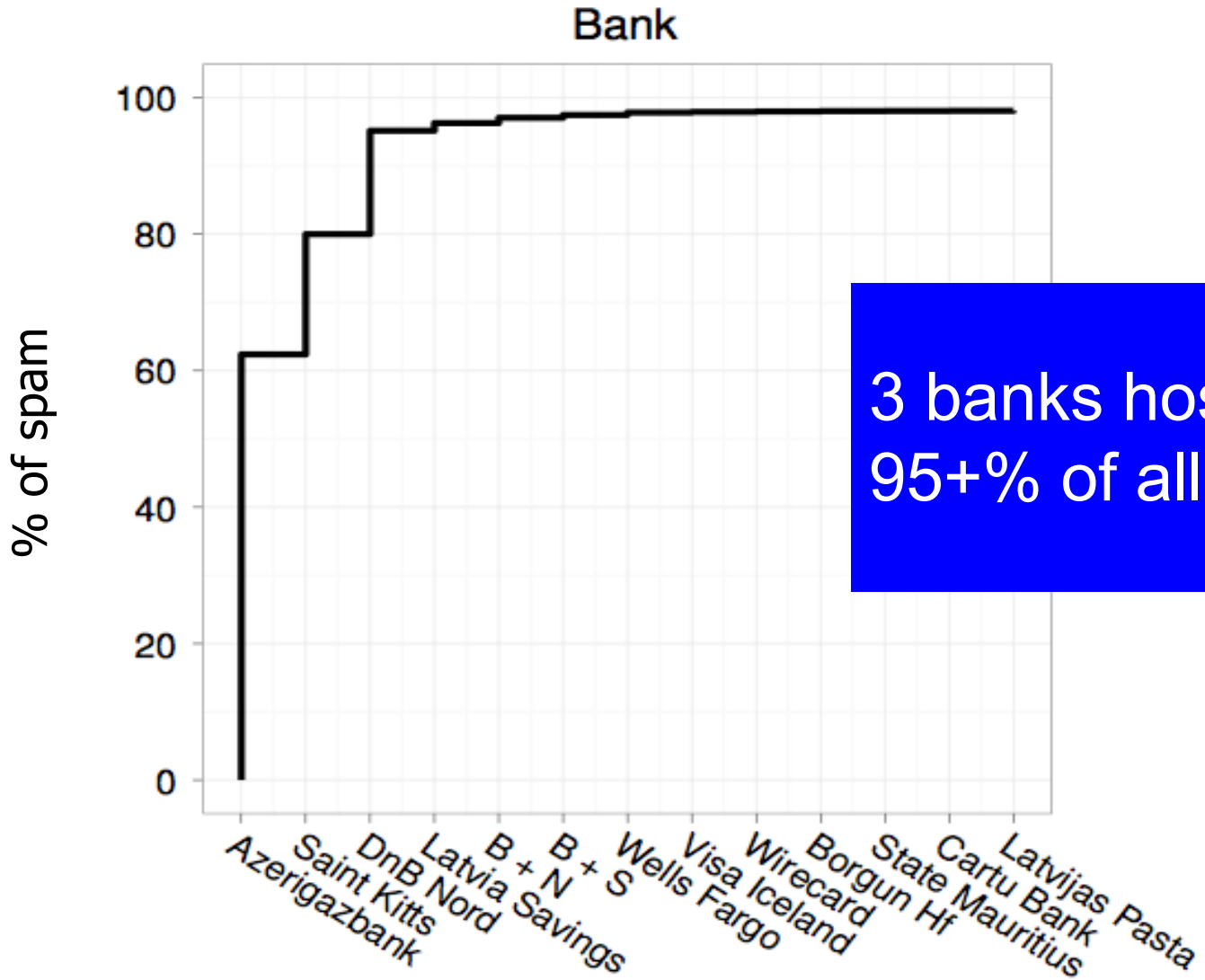
Dear **Geoff Voelker**, if you have any questions regarding your order, shipping, please contact us at:

Customers support system: www.rxsup24.com


SEALED FOR YOUR PROTECTION
vpxl
#1 Dietary Supplement for Men
100% Natural Dietary Supplement
Contains 60 capsules
hank you for using
e required


If we were to "snip" a link in this chain, which one would be the most disruptive for our least expenditure?

Merchant Bank bottlenecks



3 banks host
95+% of all sales

TWC: Frontier: Collaborative:
Beyond Technical Security: Developing an Empirical Basis for Socio-Economic Perspectives

Stefan Savage, Geoffrey M. Voelker, James Fowler, Alex Snoeren,
Lawrence Saul, Kirill Levchenko, Erin Kenneally
University of California, San Diego

Vern Paxson, Mark Allman, Chris Grier, Chris Hoofnagle, Dan Klein,
Christian Kreibich, Deirdre Mulligan, Nicholas Weaver
International Computer Sciences Institute

Damon McCoy
George Mason University

September 2012 – August 2017

TWC: Frontier: Collaborative:
Beyond Technical Security: Developing an Empirical Basis for Socio-Economic Perspectives

Stefan Savage, Geoffrey M. Voelker, James Fowler, Alex Snoeren,
Lawrence Saul, Kirill Levchenko, Erin Kenneally
University of California, San Diego

Vern Paxson, Mark Allman, Chris Grier, Chris Hoofnagle, Dan Klein,
Christian Kreibich, Deirdre Mulligan, Nicholas Weaver
International Computer Sciences Institute

Damon McCoy
George Mason University

September 2012 – August 2017

Russian Parliamentary Election

- December 5th- December 6th, 2011

Russian election protests – Saturday 10 December 2011

- Largest political event of its kind since the fall of the USSR
- An estimated 50,000 people gathered in Moscow and 10,000 in St Petersburg
- They allege widespread fraud in Sunday's polls
- More than 1,000 arrests
- Protestors pledge to take to the streets again on December 24
- They want Sunday's election results annuled

Russian Parliamentary Election

- December 5th- December 6th, 2011

- Twitter used to discuss:
  - Purported fraud, protests

- Conversations outside immediate social graph

#триумфальная
(#triumphal)

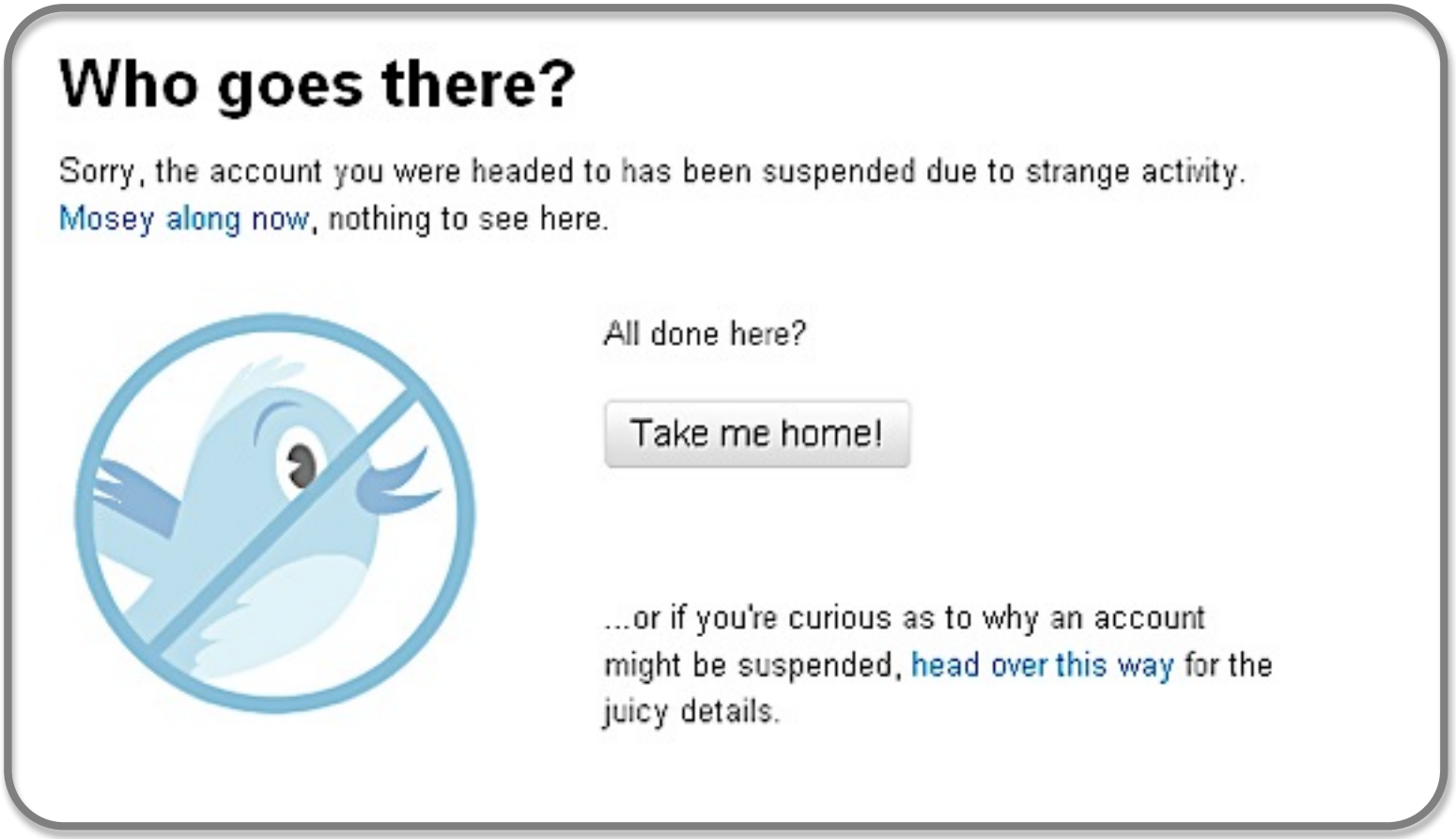
Attack

- Hashtags used by protesters swarmed by bots
  - Thousands of spam accounts
  - Spammed half a million tweets
- **Censorship**: search for hashtag only displays attack tweets
- ***Astroturfing***: hijack the sentiment of the discussion

Hashtags Attacked

Hashtag	Translation	Accounts
чп	Catastrophe	23,301
6дек	December 6th	18,174
5дек	December 5th	15,943
выборы	Election	15,082
митинг	Rally	13,479
триумфальная	Triumphal	10,816
победазанами	Victory will be ours	10,380
5dec	December 5th	8,743
навальный	Alexey Navalny	8,256
ridus	Ridus	6,116

Suspended Accounts

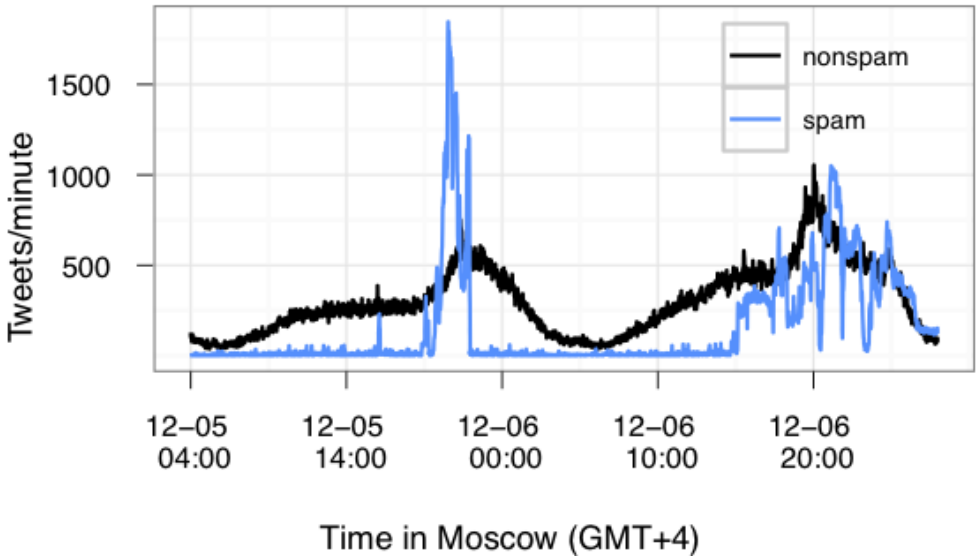


Dataset

Statistic	Suspended (Spam)	Legitimate (Nonspam)
Accounts	25,860	20,986

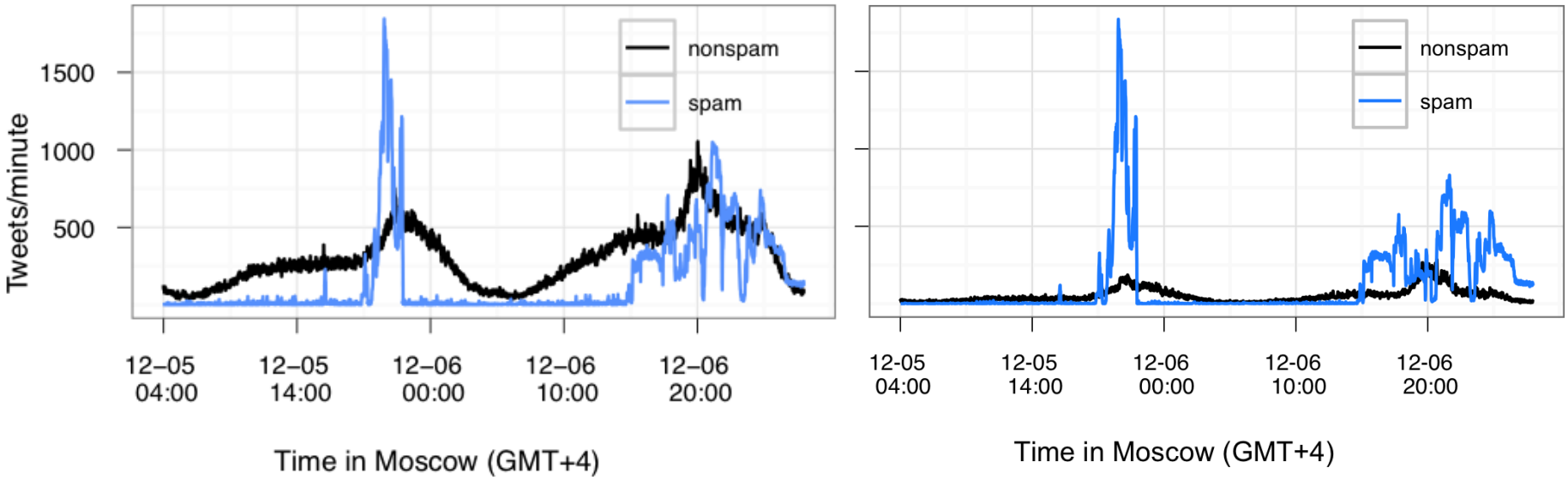
- Internal (private) Twitter data:
  - Tweet history
  - Account profiles
  - Login history
  - Search result ranking

Tweet Volume



All tweets (December 5-6, 2011) sent from accounts that discussed the election at least once

Tweet Volume



All tweets (December 5-6, 2011) sent from accounts that discussed the election at least once

Only tweets that contained attacked hashtags

Suspended Account Properties

- 99.5% are registered with *mail.ru* emails
  - 95% verified; under attacker control
- Unique IP address per registered account

Suspended Account Properties

- 99.5% are registered with *mail.ru* emails
  - 95% verified; under attacker control
- Unique IP address per registered account

- Median 122 followers, following
  - 80% of relationships to other bots

Suspended Account Properties

- 99.5% are registered with *mail.ru* emails
  - 95% verified; under attacker control
- Unique IP address per registered account

- Median 122 followers, following
  - 80% of relationships to other bots

- Registered 1 day to *7 months* in advance

Account Creation

- *Over 975,000 accounts match classifier*
  - Majority not suspended
  - 80% have 0 friends, 0 followers, 0 tweets
  - Only 4% are false positives

Account Creation

- *Over 975,000 accounts match classifier*
  - Majority not suspended
  - 80% have 0 friends, 0 followers, 0 tweets
  - Only 4% are false positives
- **Only 3% of these accounts used in attack**
- *Spam-as-a-service* program

Geolocation of Logins

Nonspam Logins

Geolocation of Logins

Nonspam Logins

Spam Logins

Compromised Hosts

- Over 11,000 unique IPs on day of attack

Compromised Hosts

- Over 11,000 unique IPs on day of attack

- Overlapping role with email spam, malware
  - 39% listed in blacklists

Compromised Hosts

- Over 11,000 unique IPs on day of attack
- Overlapping role with email spam, malware
  - 39% listed in blacklists
- Attackers intimately tied to underground economy

Where We're Going
For The Next Five Years

- Social perspectives:
  - Rise of social media as new frontier for attacks, manipulation
  - Reliance by modern attackers on (informal) social networks
    - Vulnerability to monitoring & *disruption*?
- Economic perspectives:
  - Evidence-based assessment of efficacy of defensive interventions
  - *Vulnerabilities* in the value-chain that underlies much of modern cyber "threatscape"

Where We're Going
For The Next Five Years

- Social perspectives:

Wrote one eloquent affiliate in March of this year, "Right now most affiliate eprograms have a mass of declines, cancels and pendings, and it doesn't depend much on the program IMHO, there is a general sad picture, f[redacted]ng Visa is burning us with napalm."

- Economic perspectives:
  - Evidence-based assessment of efficacy of defensive interventions
  - *Vulnerabilities* in the value-chain that underlies much of modern cyber "threatscape"