Lecture 16: Internet Abuse

Professor Adam Bates

CS 461 / ECE 422

Fall 2019

Goals for Today

- Learning Objectives:
  - Understand what makes spam possible
  - Discover how spammers make money
  - Chart the evolution of spam defenses
  - Understand phishing and advance fee fraud
- Announcements, etc:
  - **Midterm October 9th 7pm 1404 Siebel**
  - MP2 Checkpoint #2: **Due Oct 7 at 6pm**
  - MP3 Release: **Oct 7 at 6PM**
  - MP3 Checkpoint #1: **Oct 14 at 6pm**

Reminder: Please put away devices at the start of class

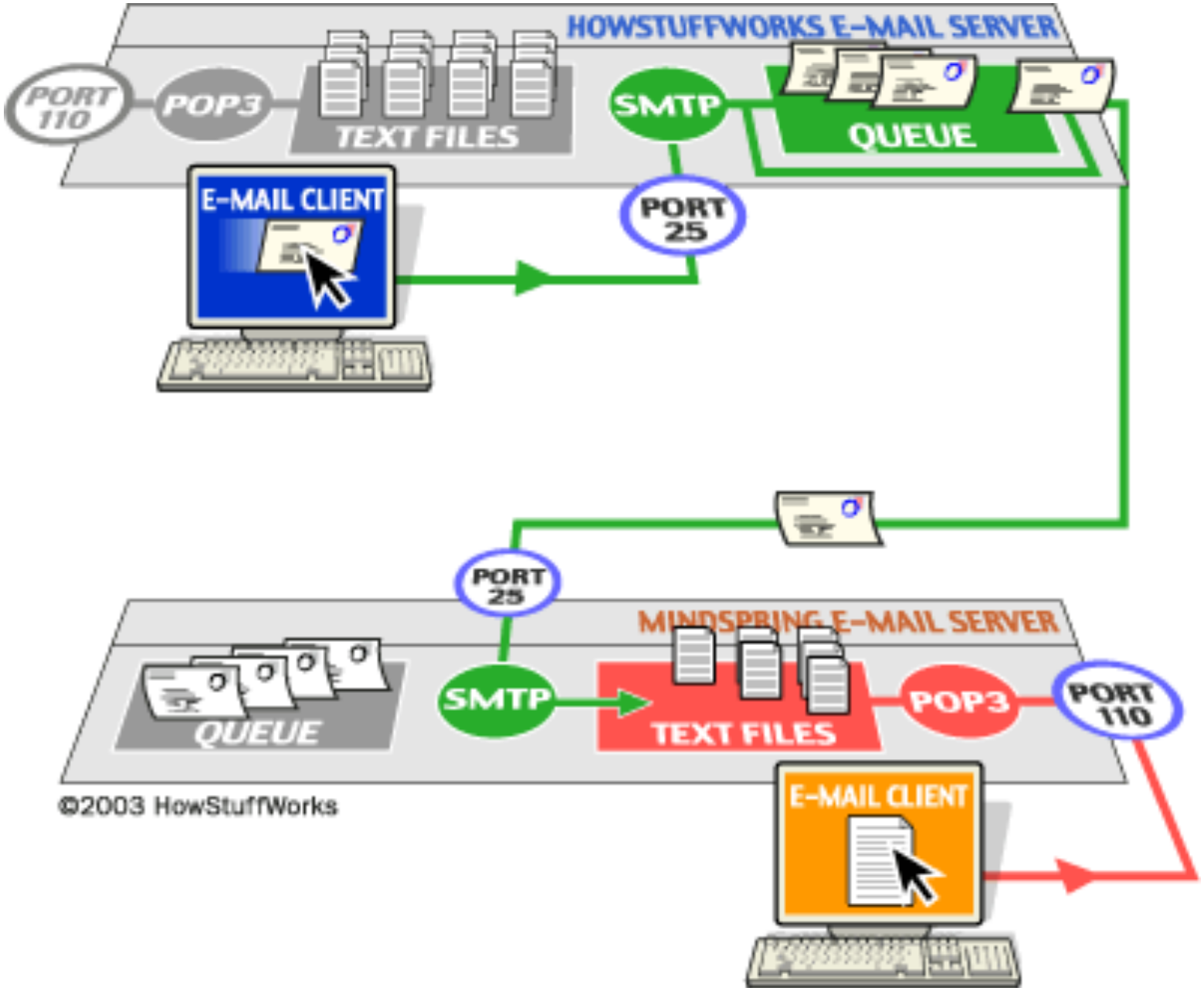
Key Concepts

- Spam
- Blacklisting
- Spam value chain
- Phishing
- Advance fee fraud
- SMTP protocol
- Pay-per-Install
- Conversion rate
- Spear phishing

How Email Works

- SMTP - Simple Mail Transfer Protocol
- POP - Post Office Protocol
- IMAP - Internet Message Access Protocol
- DNS - Domain Name System

How Email Works



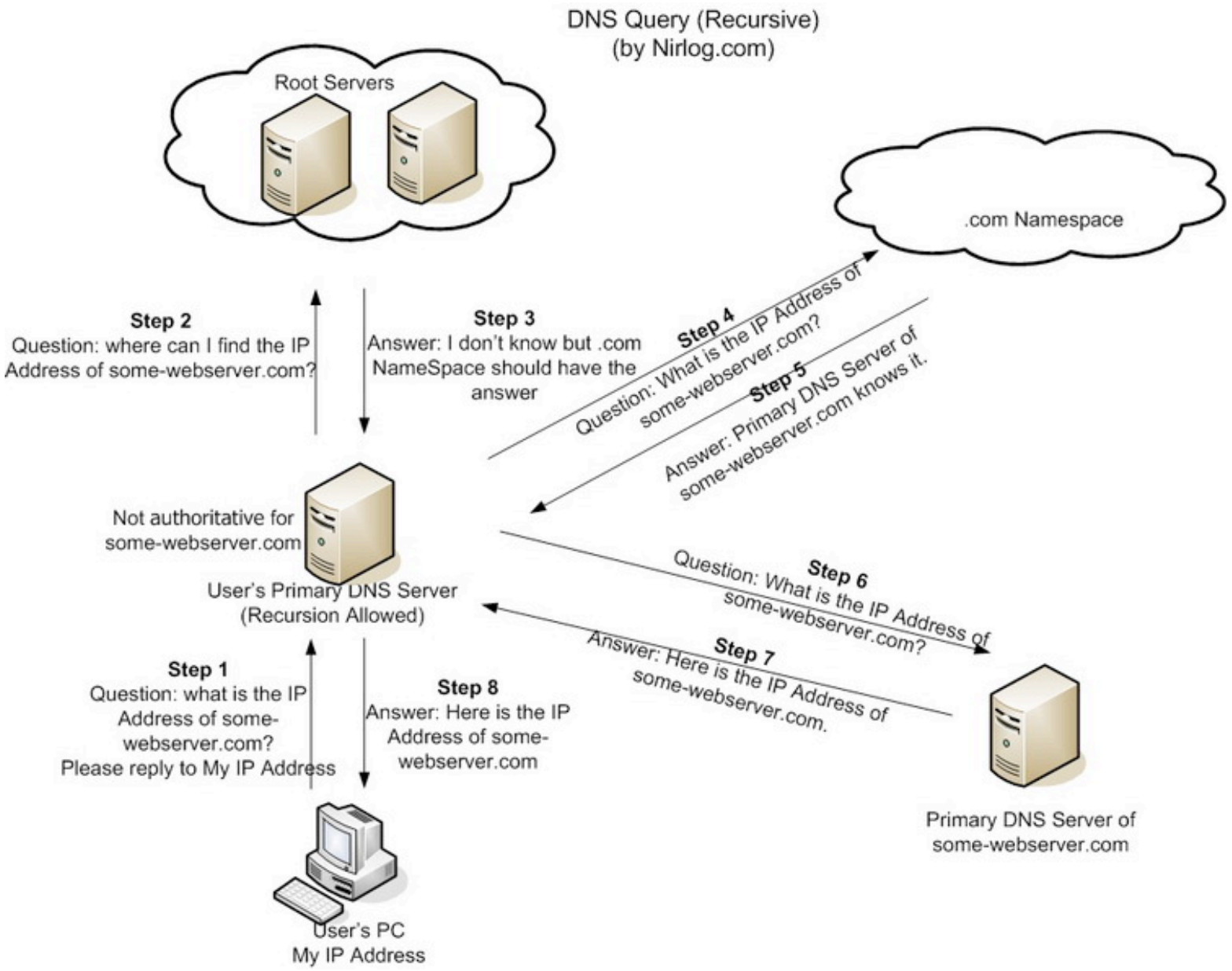
How Email Works

```
S: 220 smtp.example.com ESMTP Postfix
C: HELO relay.example.org
S: 250 Hello relay.example.org, I am glad to meet you
C: MAIL FROM:<bob@example.org>
S: 250 Ok
C: RCPT TO:<alice@example.com>
S: 250 Ok
C: RCPT TO:<theboss@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: "Bob Example" <bob@example.org>
C: To: "Alice Example" <alice@example.com>
C: Cc: theboss@example.com
C: Date: Tue, 15 Jan 2008 16:02:43 -0500
C: Subject: Test message
C:
C: Hello Alice.
C: This is a test message.
C: Your friend,
C: Bob
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
```

Where to send mail?

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61922
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 11

;; QUESTION SECTION:
;cs.ucsd.edu.          IN  MX

;; ANSWER SECTION:
cs.ucsd.edu.       43200  IN  MX  10 oec-vmmx.ucsd.edu.
cs.ucsd.edu.       43200  IN  MX  5 inbound.ucsd.edu.

;; AUTHORITY SECTION:
ucsd.edu.      43200  IN  NS  ns1.ucsd.edu.
ucsd.edu.      43200  IN  NS  ns2.ucsd.edu.
ucsd.edu.      43200  IN  NS  ns0.ucsd.edu.
ucsd.edu.      43200  IN  NS  ns1.nosc.mil.

;; ADDITIONAL SECTION:
inbound.ucsd.edu. 43200  IN  A   132.239.0.180
inbound.ucsd.edu. 43200  IN  A   132.239.0.118
oec-vmmx.ucsd.edu.    1  IN  A   132.239.8.22
oec-vmmx.ucsd.edu.    1  IN  A   132.239.8.20
oec-vmmx.ucsd.edu.    1  IN  A   132.239.8.21
```

DNS


DNS Query (Recursive)
(by Nirlog.com)
Root Servers
.com Namespace
Step 2
Question: where can I find the IP Address of some-webserver.com?
Step 3
Answer: I don't know but .com NameSpace should have the answer
Step 4
Question: What is the IP Address of some-webserver.com?
Step 5
Answer: Primary DNS Server of some-webserver.com knows it.
Not authoritative for some-webserver.com
User's Primary DNS Server
(Recursion Allowed)
Step 6
Question: What is the IP Address of some-webserver.com?
Step 7
Answer: Here is the IP Address of some-webserver.com.
Step 1
Question: what is the IP Address of some-webserver.com?
Please reply to My IP Address
Step 8
Answer: Here is the IP Address of some-webserver.com
Primary DNS Server of some-webserver.com
User's PC
My IP Address

Spam, Gen 1

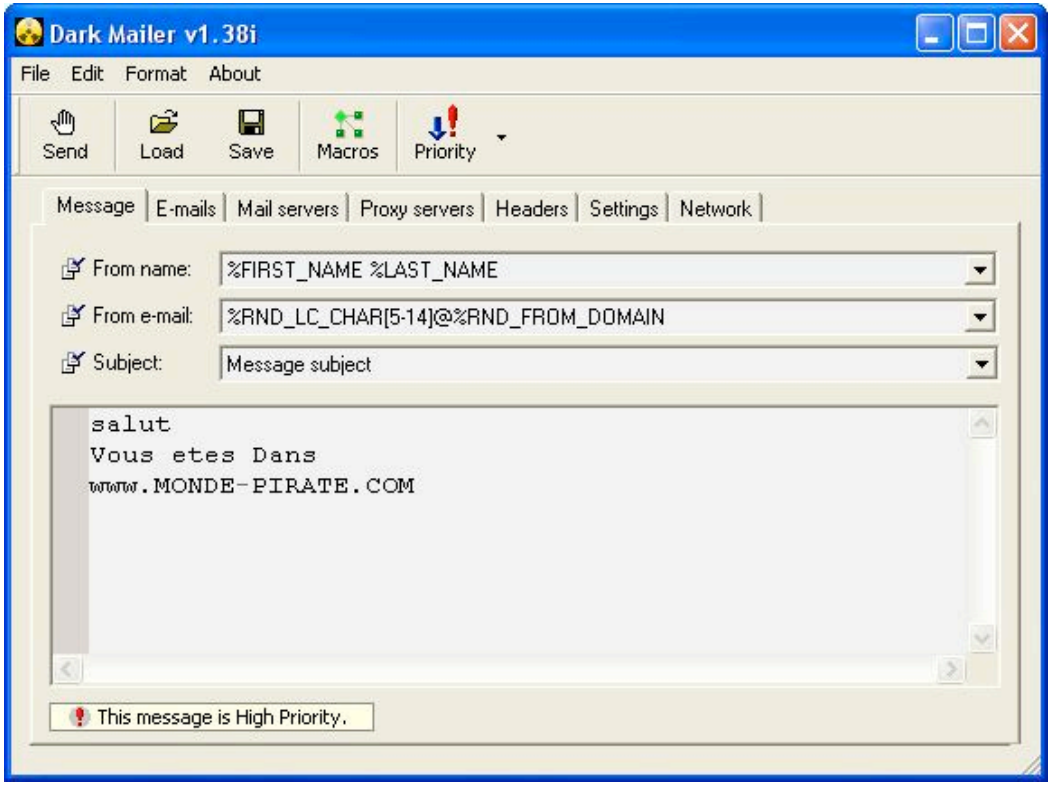
- Send spam directly to users via SMTP

Spam, Gen 1

- Send spam directly to users via SMTP
- **Defense**: Blacklist known spam message content
- **Defense**: Blacklist hosts that spam

Spam, Gen 2

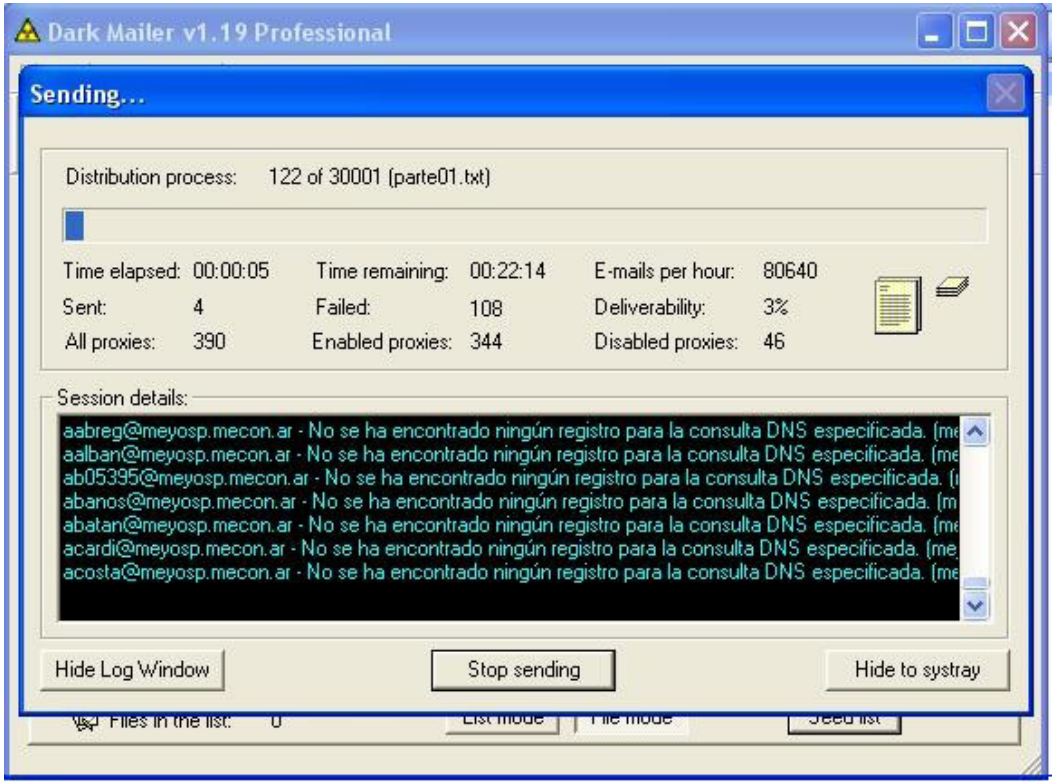
- Send spam via SMTP proxies
- Modify messages in minor ways



Further reading: Henry Stern. "A Survey of Modern Spam Tools." *CEAS 2007.*

Spam, Gen 2

- Send spam via SMTP proxies
- Modify messages in minor ways



Further reading: Henry Stern. "A Survey of Modern Spam Tools." *CEAS 2007.*

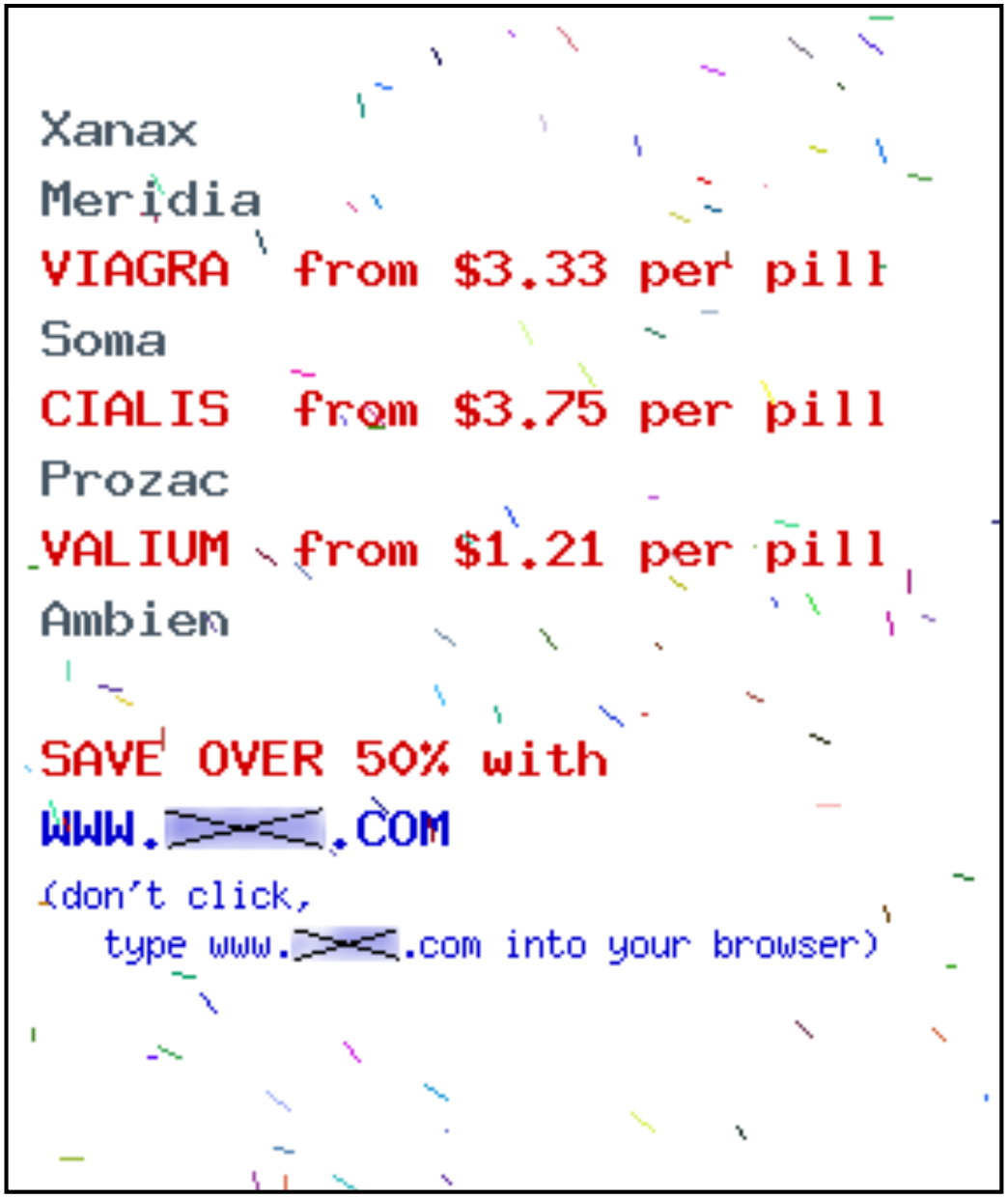
Spam, Gen 2

- Send spam via SMTP proxies
- Modify messages in minor ways
- **Defense**: Modify signatures; use n-gram analysis to attempt to learn templates.

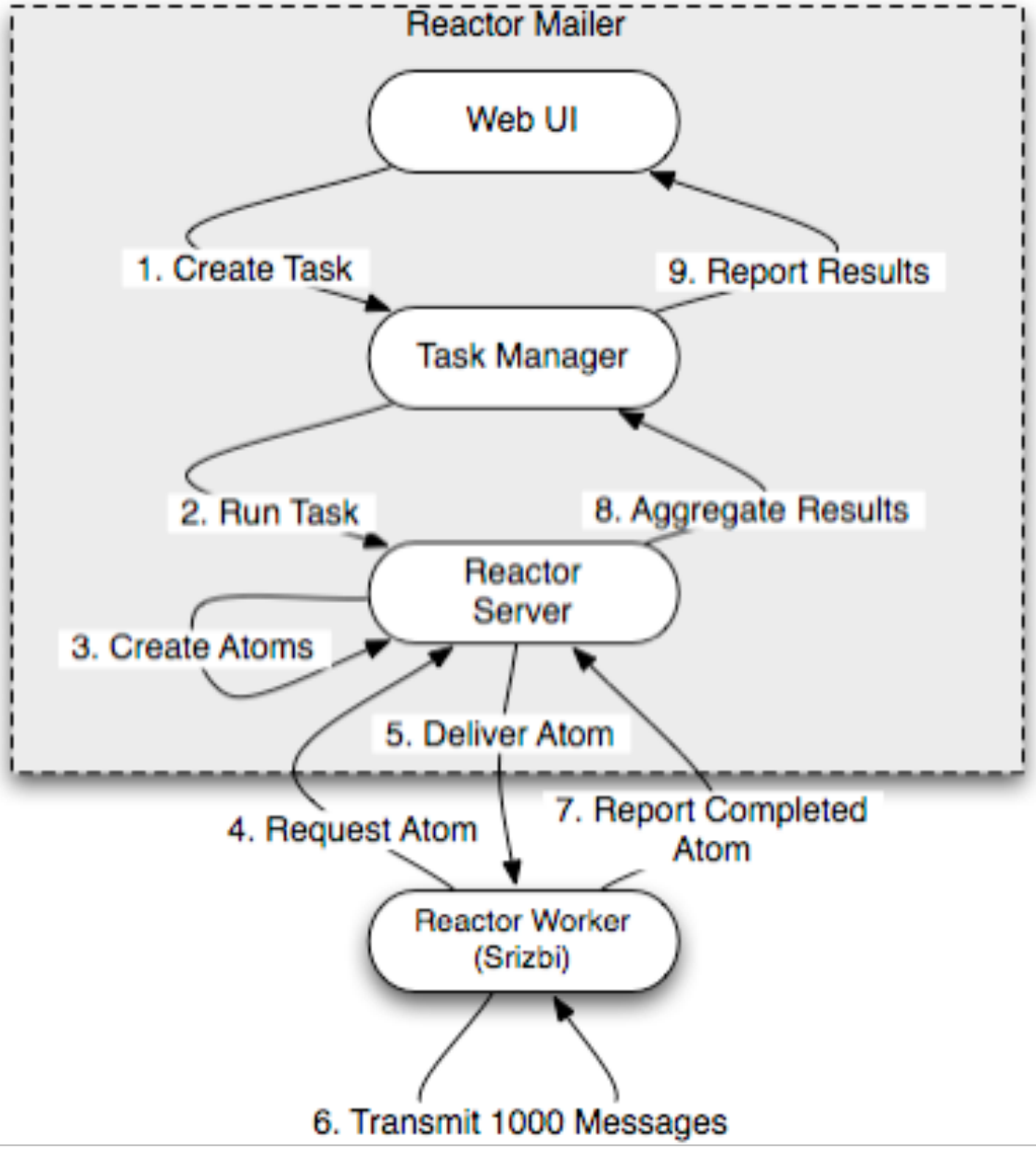
Further reading: Henry Stern. "A Survey of Modern Spam Tools." *CEAS 2007.*

Spam, Gen 3

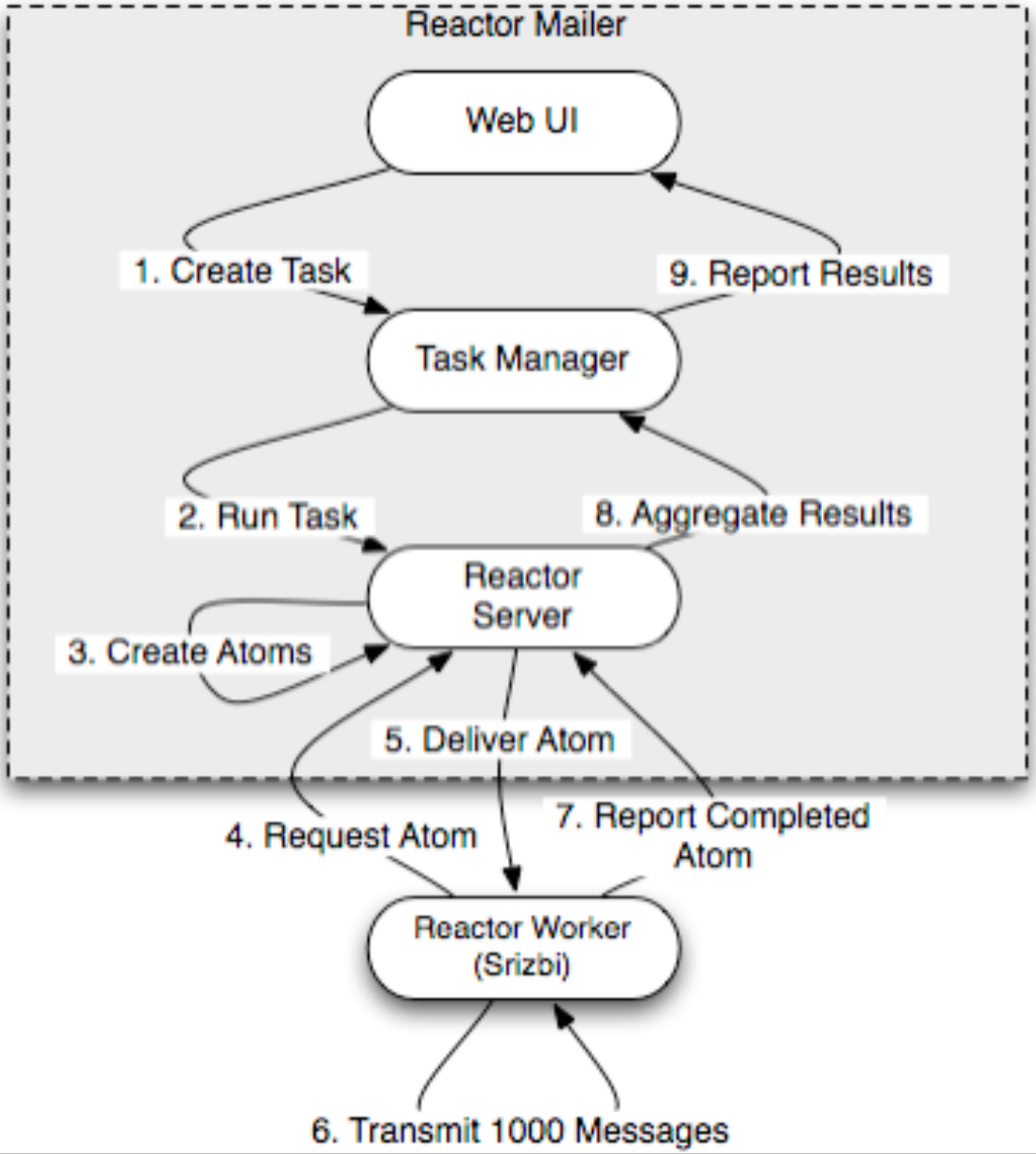
- Send via botnet (plain SMTP)
- Modify messages more aggressively
- Avoid spam keywords (e.g. "viagra")
  - Inuendo: "Excellent hardness is easy"
- Image spam



Spam, Gen 3


Reactor Mailer
Web UI
1. Create Task
9. Report Results
Task Manager
2. Run Task
8. Aggregate Results
Reactor Server
3. Create Atoms
5. Deliver Atom
4. Request Atom
7. Report Completed Atom
Reactor Worker (Srizbi)
6. Transmit 1000 Messages

Spam, Gen 3



Macro	Description
{set VAR= MACRO}	Set the value of a variable.
{static VAR}	Substitute the value of a variable.
{rndabc L1,L2}	Random english text with variable size (from L1 to L2, in example {rndabc 5,8}).
{rnddig L1,L2}	Random digits line with variable size (from L1 to L2).
{rnddigabc L1,L2}	Random english text and digits line with variable size (from L1 to L2).
{rndru L1,L2}	Random Cyrillic text with variable size.
{rndrugl L1,L2}	Random Cyrillic vowels with variable size.
{rndrusogl L1,L2}	Random Cyrillic consonants with variable size.
{hex_up X}, {hex_down X}	Random hexadecimal digits, upper and lower case respectively.
{rndsyn word1,word2,word3}	Random word from set.
{rndline filename}	Random line from file filename.
{rndbody filename1,...,filenameN}	Random file content from set.
{shuffle word1,...,word3}	Randomly shuffled words word1, ..., word3, without separators. Similar functions using other separators.
{fuzzy any text you want}	Exchange two random adjacent letters in each word.
{from_domain filename}	Bot's provider domain address, or, of domain not available, random line from file filename.
{sender_dom}	Domain from "From:" mailing address, which used in message.
{sender_addr}	Address from "From:" mailing address, which used in message.
{sender_name}	Sender name from "From:" mailing address, which used in message.
{receiver_dom}	Receiver domain from "To:" mailing address, which used in message.
{receiver_addr}	Receiver address from "To:" mailing address, which used in message.
{receiver_name}	Receiver name from "To:" mailing address, which used in message.
{server_mx}	Receiver IP.
{proxy_ptr}	Proxy IP.
{proxy_addr}	Proxy address.
{attach_name N}	Random name of attached file.
{attach_cid N}	Random CID of attached file.
{date}	Current date.
{datetime}	Current date and time.
{tm_year X}	Current year, 4 digits. Similar functions for other granularities.
{imgtext X}	Insert a "text image" described in section 2.3.

Where do spam clients come from?

- Answer: Botnets

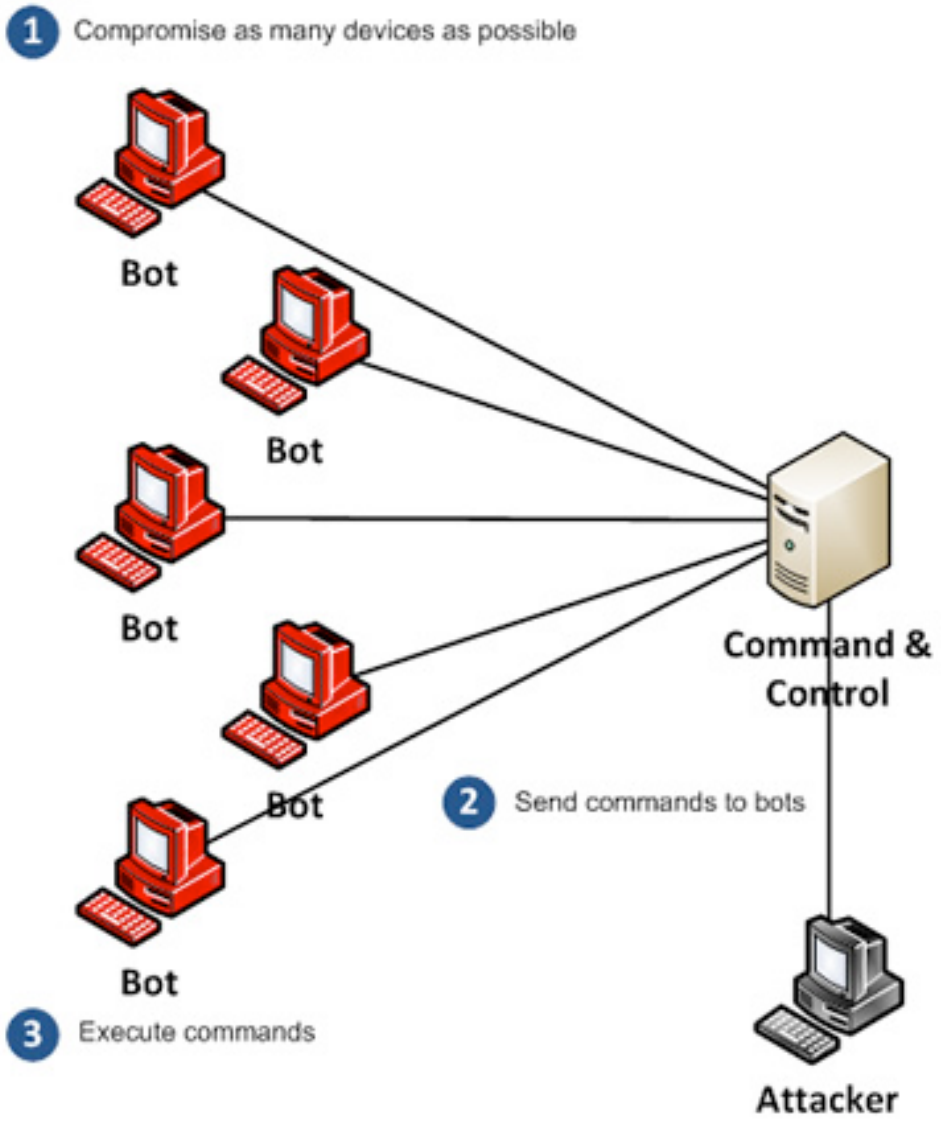
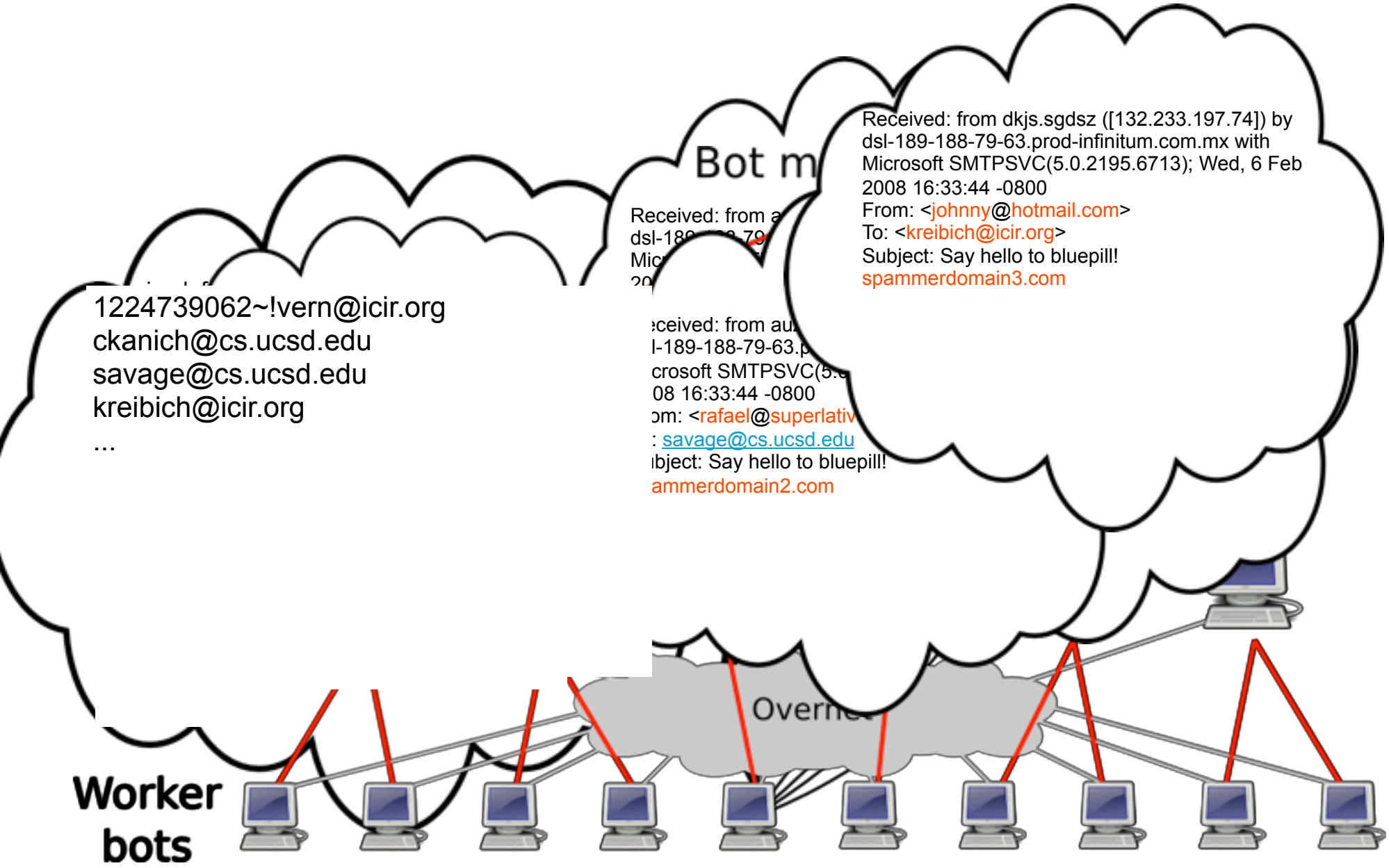


Image: DELL SecureWorks

The Storm Botnet



Where do bots come from?

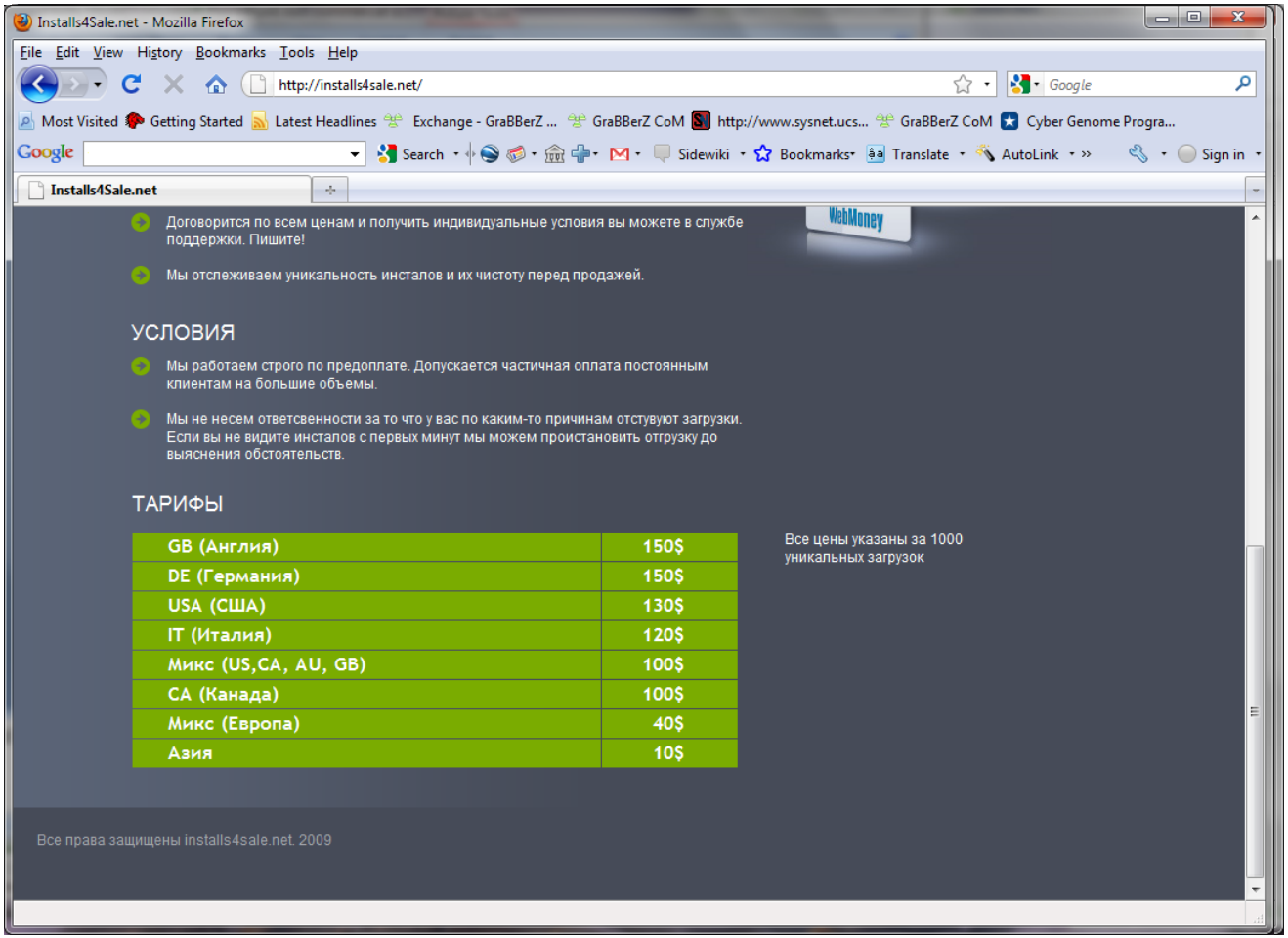
- **Old model:** infection campaigns
  - E.g.: Storm's ecard campaigns

Where do bots come from?

- **Newer model:** Pay-per-install
  - E.g. Rustock botnet

Where do bots come from?

- **Newer model:** Pay-per-install
  - E.g. Rustock botnet

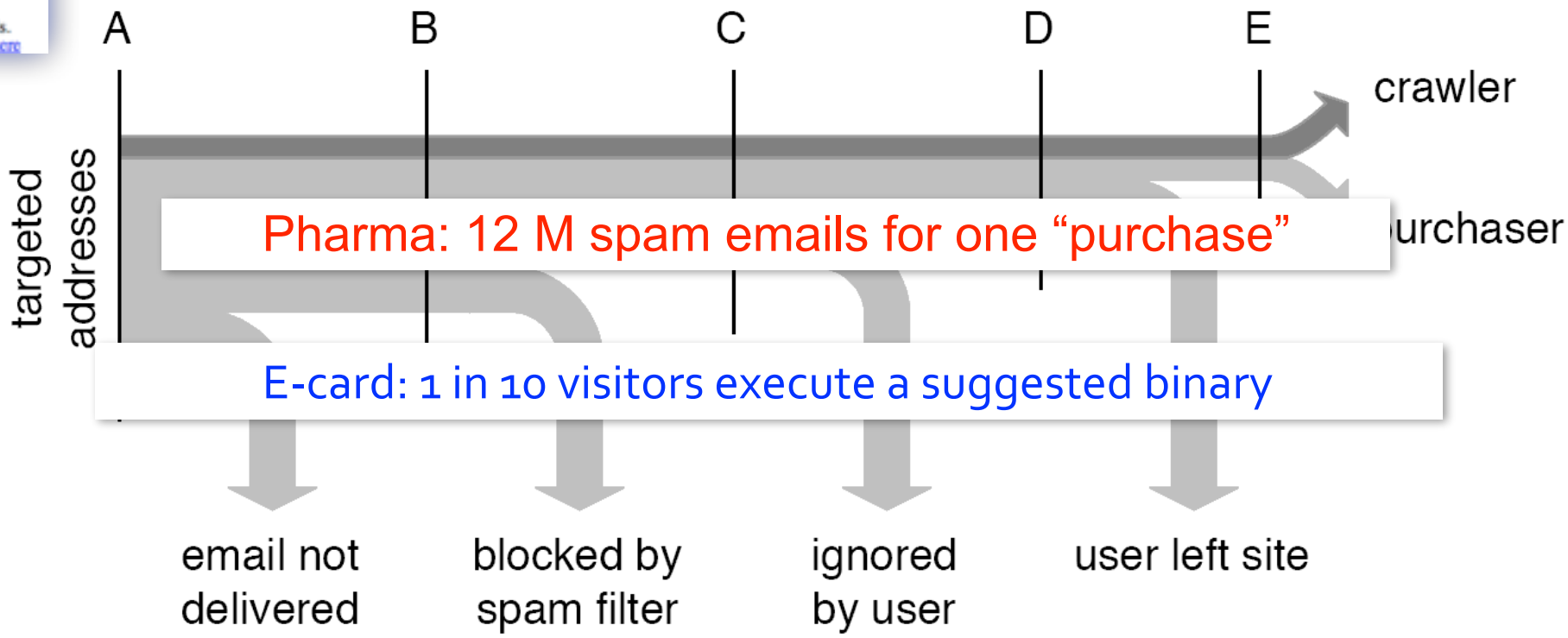


Spam, Gen 4

- Send via Web mail
- Send via authenticated SMTP
- Simpler messages

Spam, Gen 4

Sent	MTA	Inbox	Visits	Conversions
347.5M	82.7M (24%)		10,522 (0.003%)	28 (0.000008%)
83.6 M	21.1M (25%)		3,827 (0.005%)	316 (0.00037%)
40.1 M	10.1M (25%)		2,721 (0.005%)	225 (0.00056%)



How can we prevent spam?

- **Problem**: Prevent spam
- **Solution?** Stop spam by blocking spam delivery
  - Led to arms race
  - More annoying spam
  - More expensive filters
- Still, spam exists. Therefore, it must is profitable
- Monetizing spam is a complex operation …
  - … is delivery really the best place to stop spam?

Spam Value Chain

- Step 1: Send Spam
- Step 2: ???
- Step 3: Profit??
- **Spam value chain**: The sequence of steps through which a spam message is converted into revenue

Spam Value Chain

1. **Advertising**

   Getting message to user (Spamalytics '08)

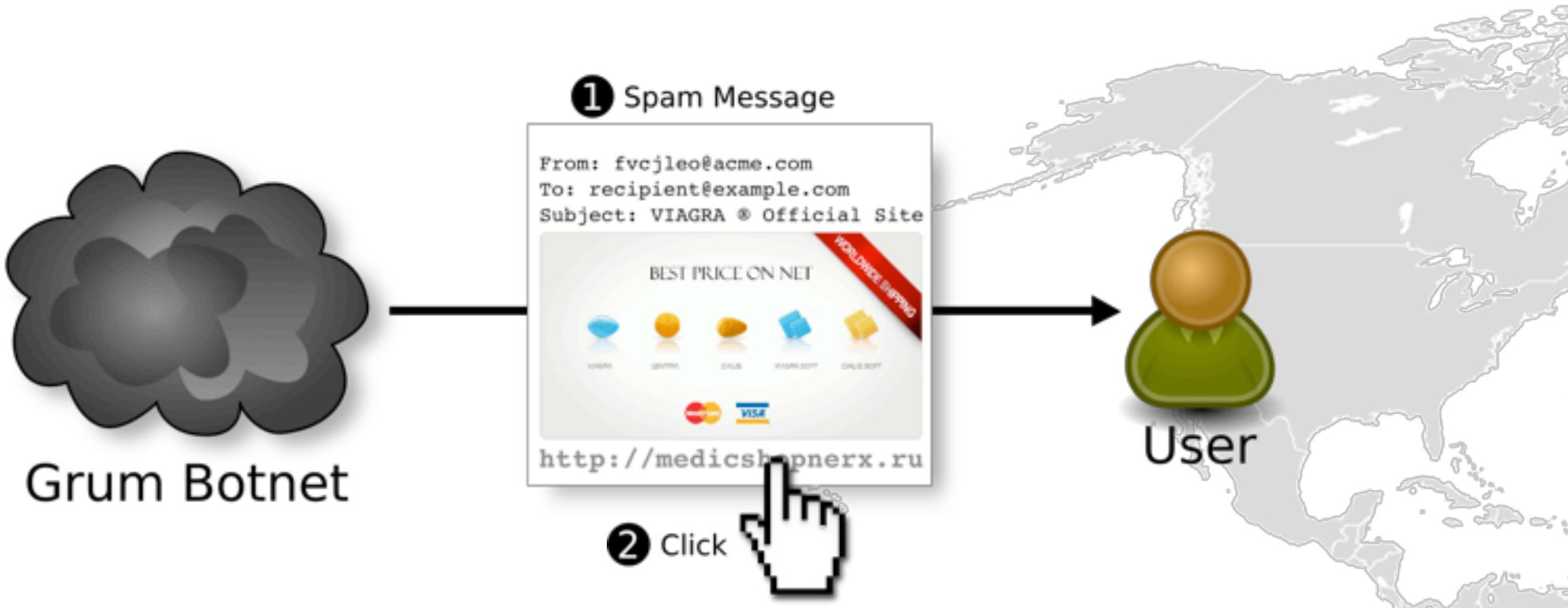
2. **Click support**

   Making it possible for user to act

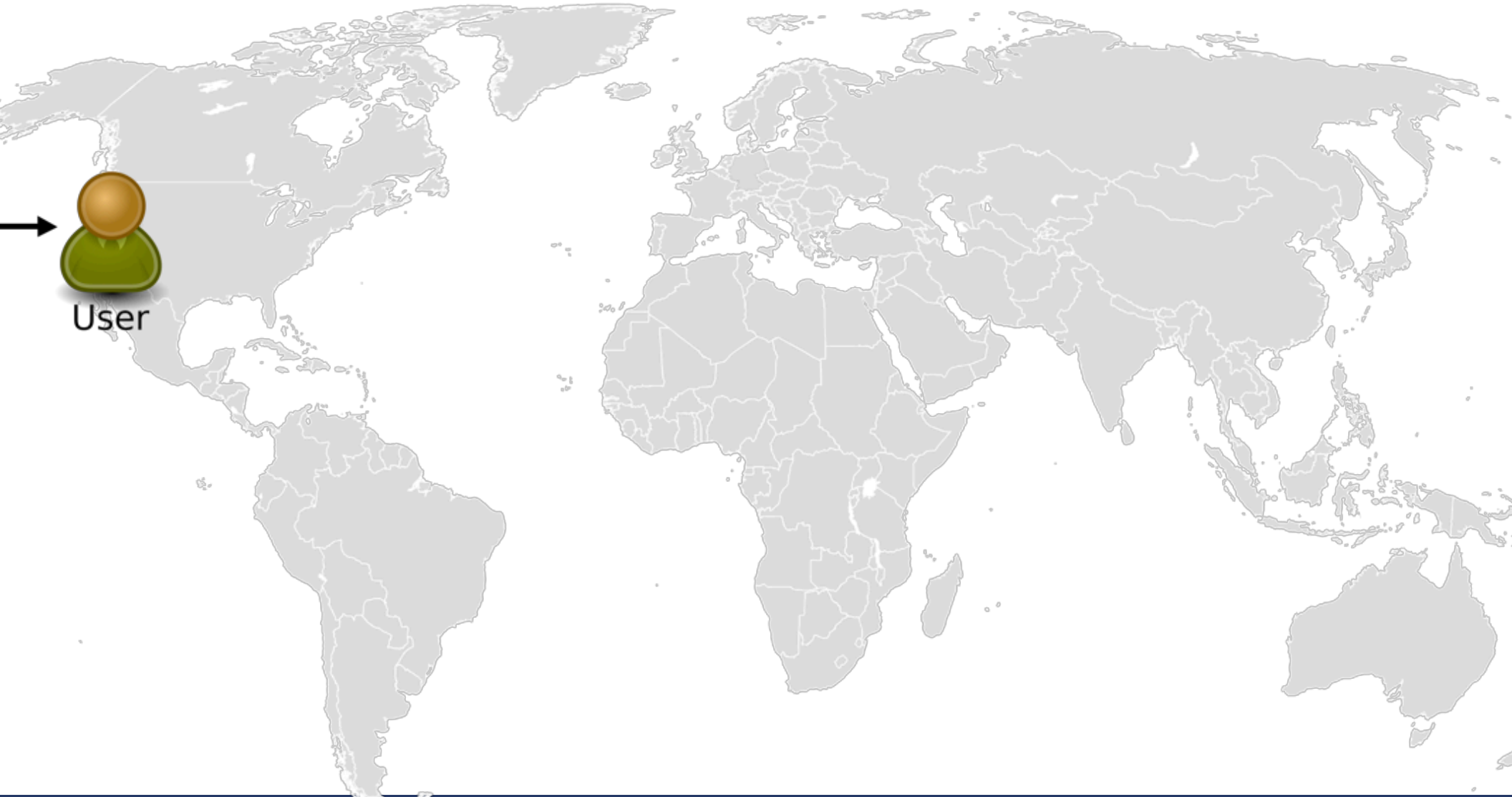
3. **Conversion**

   Turning user action into money

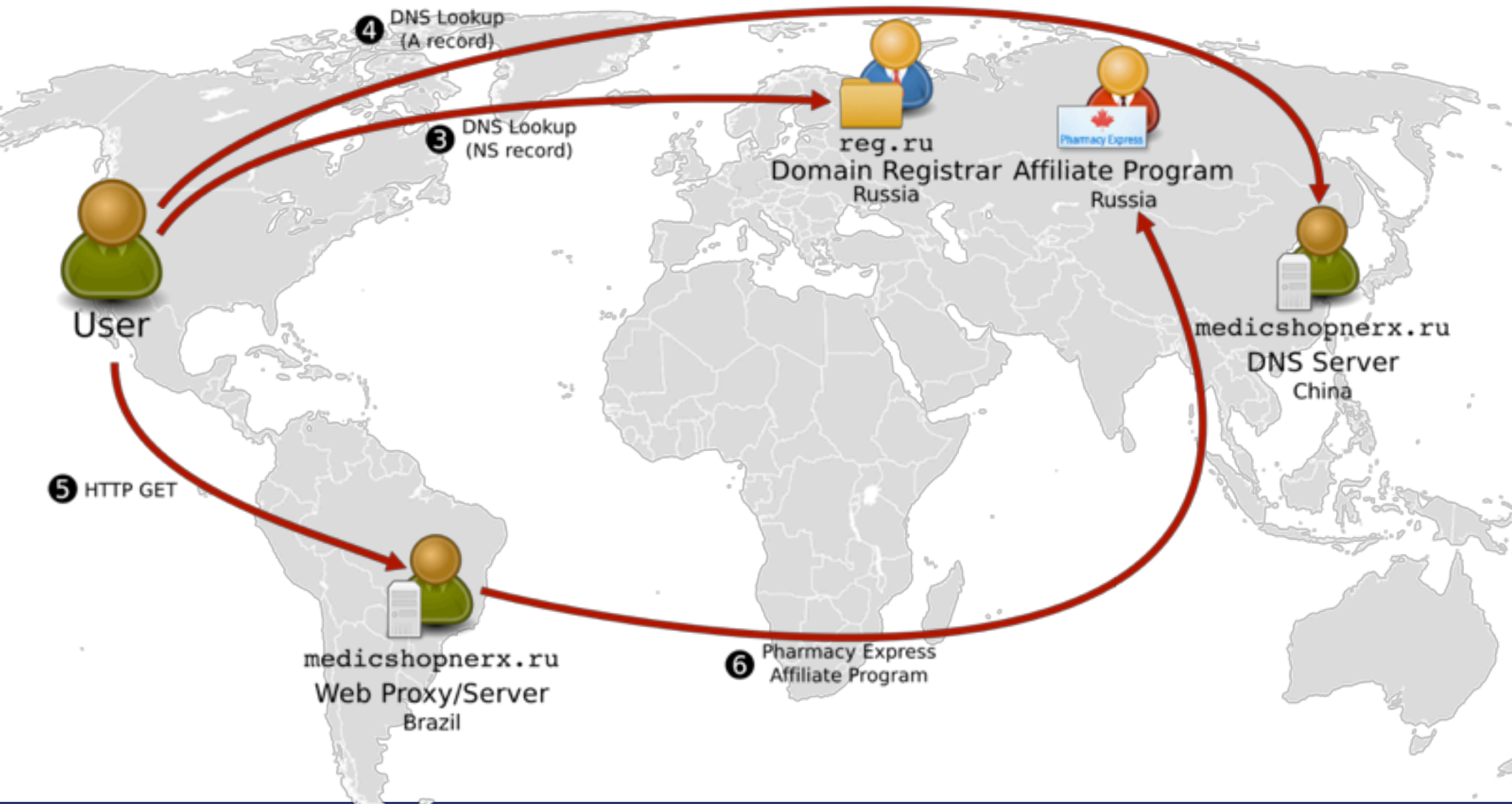
Spam Value Chain



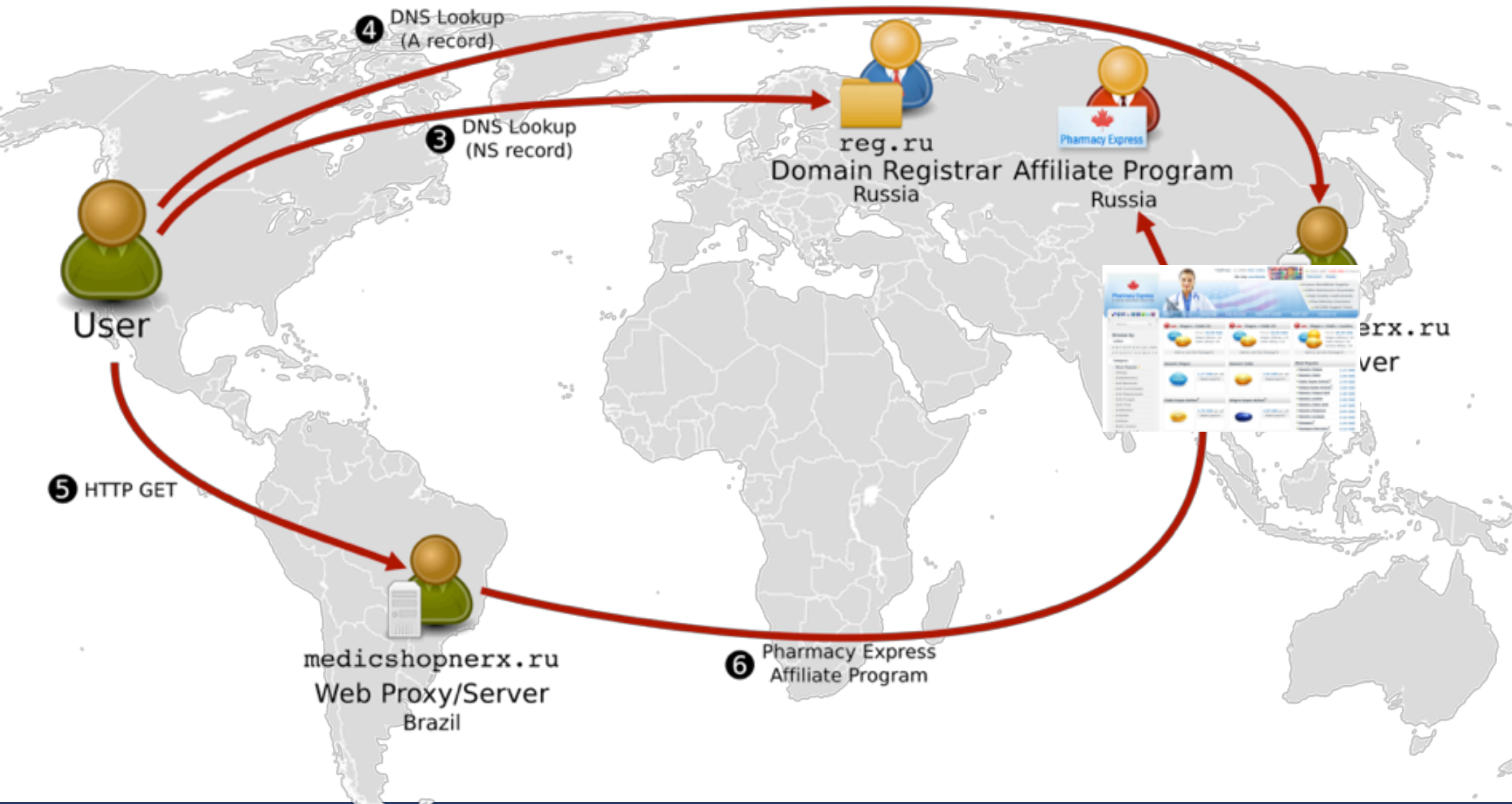
Spam Value Chain



Spam Value Chain



Spam Value Chain



Affiliate Programs

- Handle logistics
  - Storefront, payment, fulfillment
- Pay a commission
- Let spammer focus on spamming

Affiliate Programs

Преимущества RX-Promotion

Партнерская программа RX-Promotion создает все условия для выгодной, комфортной и интересной работы. Думаете это просто слова? Нет, это вполне конкретные преимущества:

Высокая п

В рамках партнерск ете зарабатывать вплоть сделки и до 15% от участника. Эти цифр

UP TO 60%
COMMISSION

Выплаты по требованию

Постоянным партнерам гарантируются практически мгновенное перечисление денег безо всяких задержек и проволочек, а также отсутствие необходимости оставлять залоговую сумму. Выплаты производятся точно, стабильно и оперативно.

Bestsellers

Viagra
Only: $ 0.99

Viagra (Sildenafil) It has been estimated that impotence affects 140 million men worldwide. Over half of all men with impotence are ...

Cialis
Only: $ 1.99

Cialis (TADALAFIL) is an oral drug, used for treating male impotence, also known as erectile men's erectile dysfunction. Clinical ...

Female Viagra
Only: $ 2.65

Female Viagra represents a serious approach to the problem of female sexual arousal disorder (FSAD) and female sexual dysfunction ...

Viagra Professional
Only: $ 3.50

Unlike previously approved treatments for impotence, Viagra does not directly cause penis erection, but affects the response to sexual ...

Cialis Professional
Only: $ 4.01

Cialis Professional (Tadalafil) is newly formulated and chemically improved prescription medicine has proved to be useful for ...

Viagra Super Active
Only: $ 2.45

Viagra Super Active (SILDENAFIL) is a new therapy for the treatment of erectile dysfunction. This super-active formulation gives the ...

Cialis Super Active
Only: $ 3.30

Cialis Super Active (TADALAFIL) is a newly formulated and

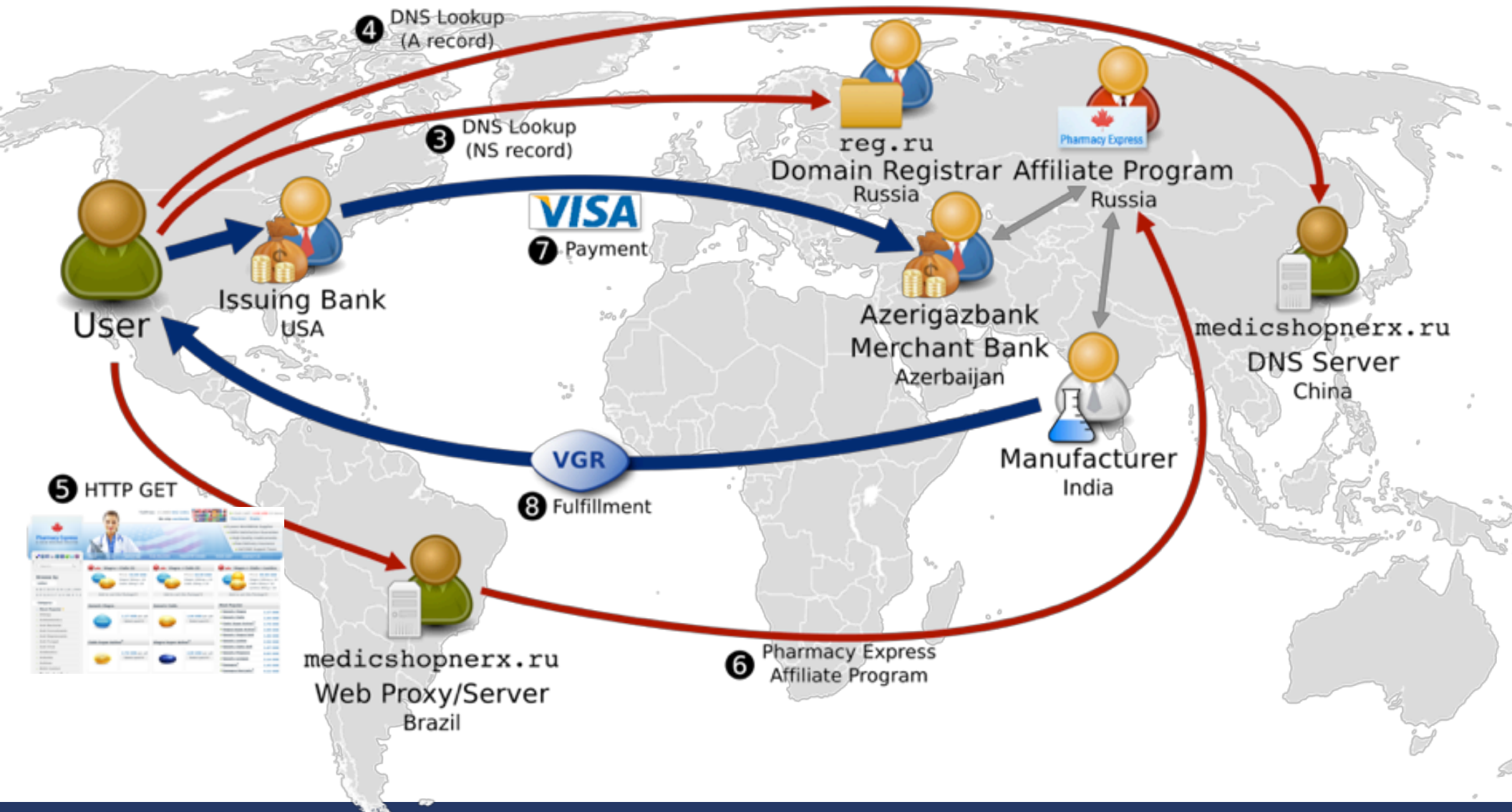
Cialis Soft
Only: $ 3.32

Generic Cialis Soft (TADALAFIL SOFT) is a phosphodiesterase inhibitor used for the

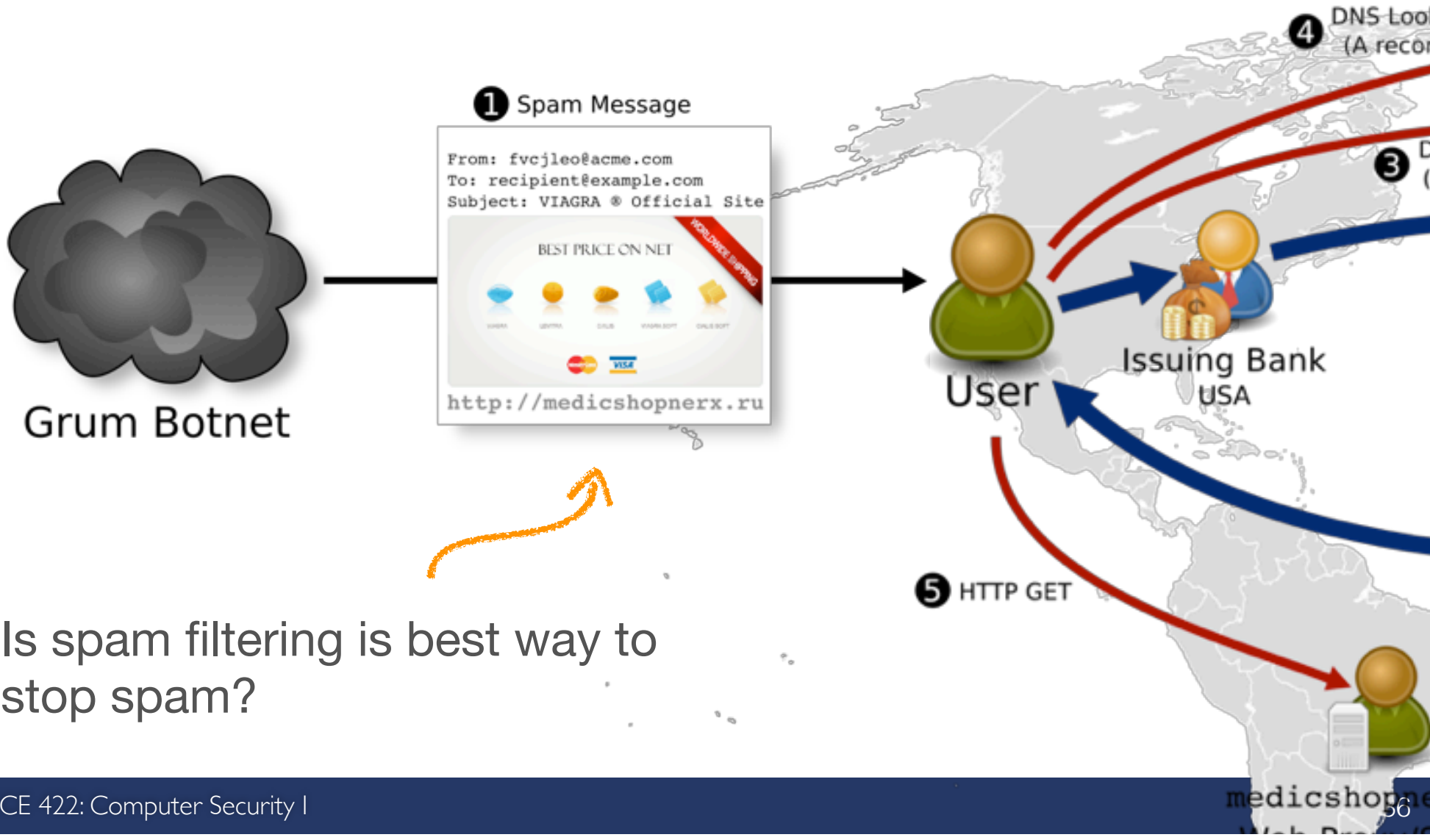
Viagra Soft
Only: $ 1.87

Sildenafil (Viagra) Citrate are the revolutionary treatment drugs for men suffering from

Spam Value Chain

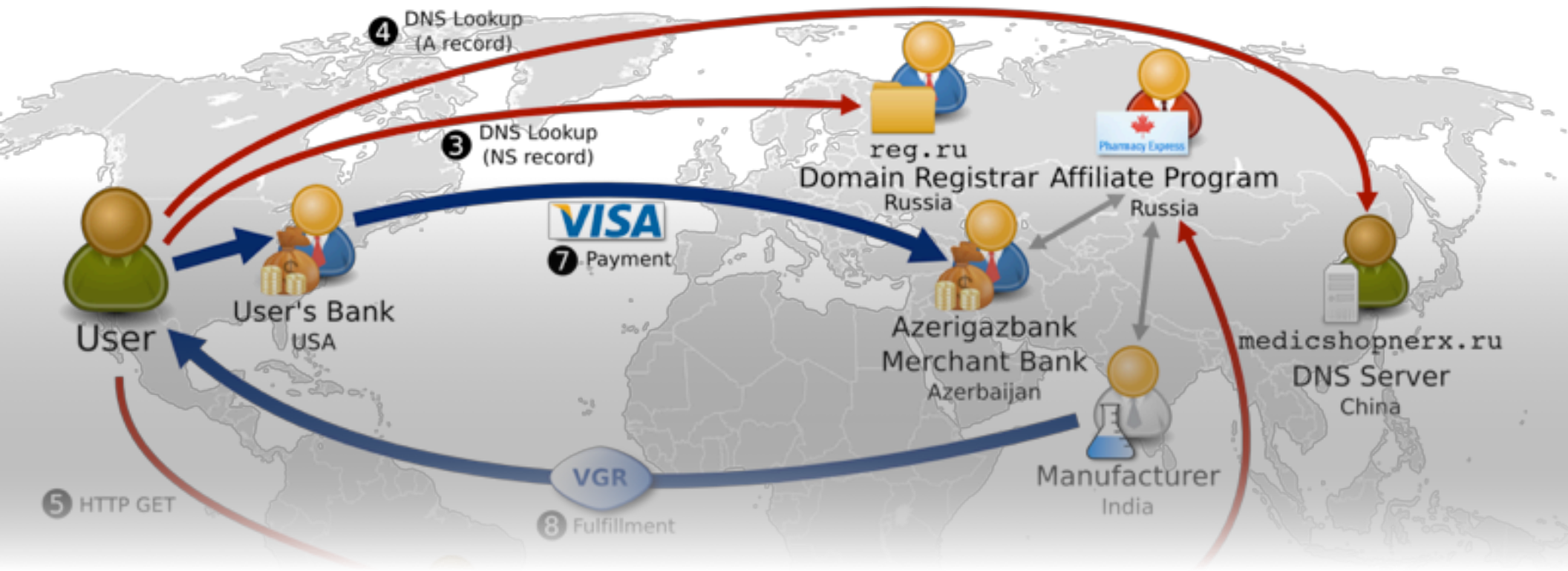


Spam Value Chain



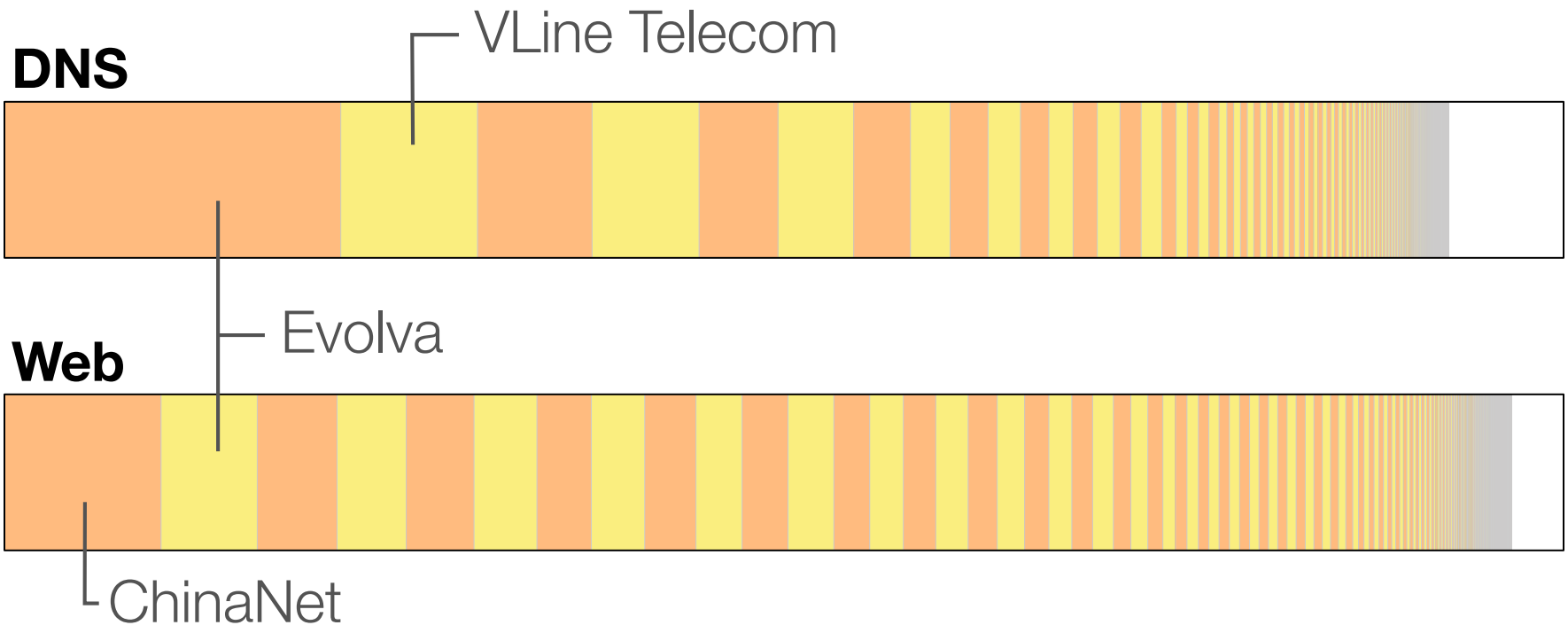
- Is spam filtering is best way to stop spam?

Points of Intervention



Levchenko et al. *"Click Trajectories: End-to-End Analysis of the Spam Value Chain", IEEE S&P 2011.*

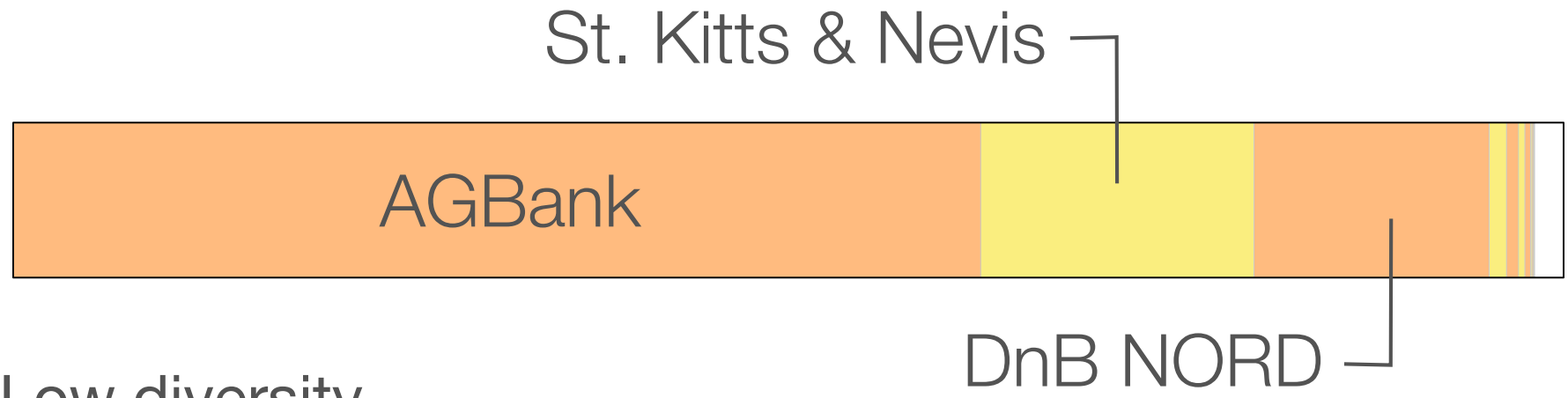
Hosting



- Many choices
- Low switching cost (change servers and update DNS)

Levchenko et al. *"Click Trajectories: End-to-End Analysis of the Spam Value Chain", IEEE S&P 2011.*

Merchant Banks



- Low diversity
  - Three banks cover 95% of our corpus
  - Few banks willing to work with "high risk" merchants
- High switching cost
  - Need to create merchant account at a bank in person
  - Bank holds money to cover contested charges

Levchenko et al. *"Click Trajectories: End-to-End Analysis of the Spam Value Chain", IEEE S&P 2011.*

How can we prevent spam?

- Disrupting spam means disrupting a business process
- **Insight**: Payment processing weakest part of value chain
  - Low diversity, high switching cost

Levchenko et al. *"Click Trajectories: End-to-End Analysis of the Spam Value Chain", IEEE S&P 2011.*

Phishing Spam

- **Phishing**: Convince victim to reveal secret information (usually password) via email by impersonating legitimate authority
- **Spear phishing**: Targeted phishing that use additional knowledge of target

Phishing Spam

From: HELP DESK <etty@unpad.ac.id>
Date: Sat, Jul 24, 2010 at 03:31
Subject: Your mailbox has exceeded the storage limit
To:

Dear mail user,

This is to inform you that Your mailbox has exceeded the storage limit
which is20GB as set up by our administrator service center,you are currently
running on 20.9GB,To re-validate your mailbox please fill the form and send to our system administrator
center.
First Name: (.....)
Last Name.....)
Email Address.....)
user name(.....)
password(.....)
confirm password(.....)
To increase your mail size,We apologize for any inconvenience. Thank you for your anticipated
co-operation.
Note: Failure to comply may result lose of your account within 24 hours.
Thanks. System Administrator center .

_____
misc mailing list
misc@cs.ucsd.edu
https://csemail.ucsd.edu/mailman/listinfo/misc

Passwords

Classify Your Data Passwords Phishing Social Media Safety Contact

A strong, well-protected password is one of the most crucial components of computer security. Strong passwords not only protect your machine from unauthorized access, but also protects your data within and across websites you use. It is important to have a series of strong passwords and to avoid using the same password on more than one account (i.e. don't use the same password for your Facebook and bank accounts). Technology Services strongly recommends using a password management tool, both to help you store your passwords and also to assist in creating strong passwords.

Learn how to make a strong password: https://answers.uillinois.edu/illinois/page.php?id=69112

g password. https://answers.uillinois.edu/illinois/page.php?id=65112

r password, you can visit https://identity.uillinois.edu

nplemented two-factor authentication to further secure some University-related
entication provides added security as it requires the customer to have a second device
e to confirm the identity of the person attempting to log in.

ollowing these steps:

password.
ord with anyone else in person, by email, or online. It's against campus policy to let
r password. IT staff will never ask you for your password, particularly by email.
rs to your password reset questions with anyone.
that you use for highly sensitive accounts such as your email, your bank account, your
niversity of Illinois account.
ord or the answers to your password reset questions on publicly viewable web sites,
l media profiles.
s to your password reset questions in any public settings. This includes pictures of your
s your reset question.

From: "Patterson, Sandra K" <skpttrsn@illinois.edu>
Subject: **Information service**
Date: March 25, 2019 8:33:44 AM CDT

Notification of Ticket Escalation

Workspace: Service Desk
Ticket: Request closed
Request Number: #135863CCO223

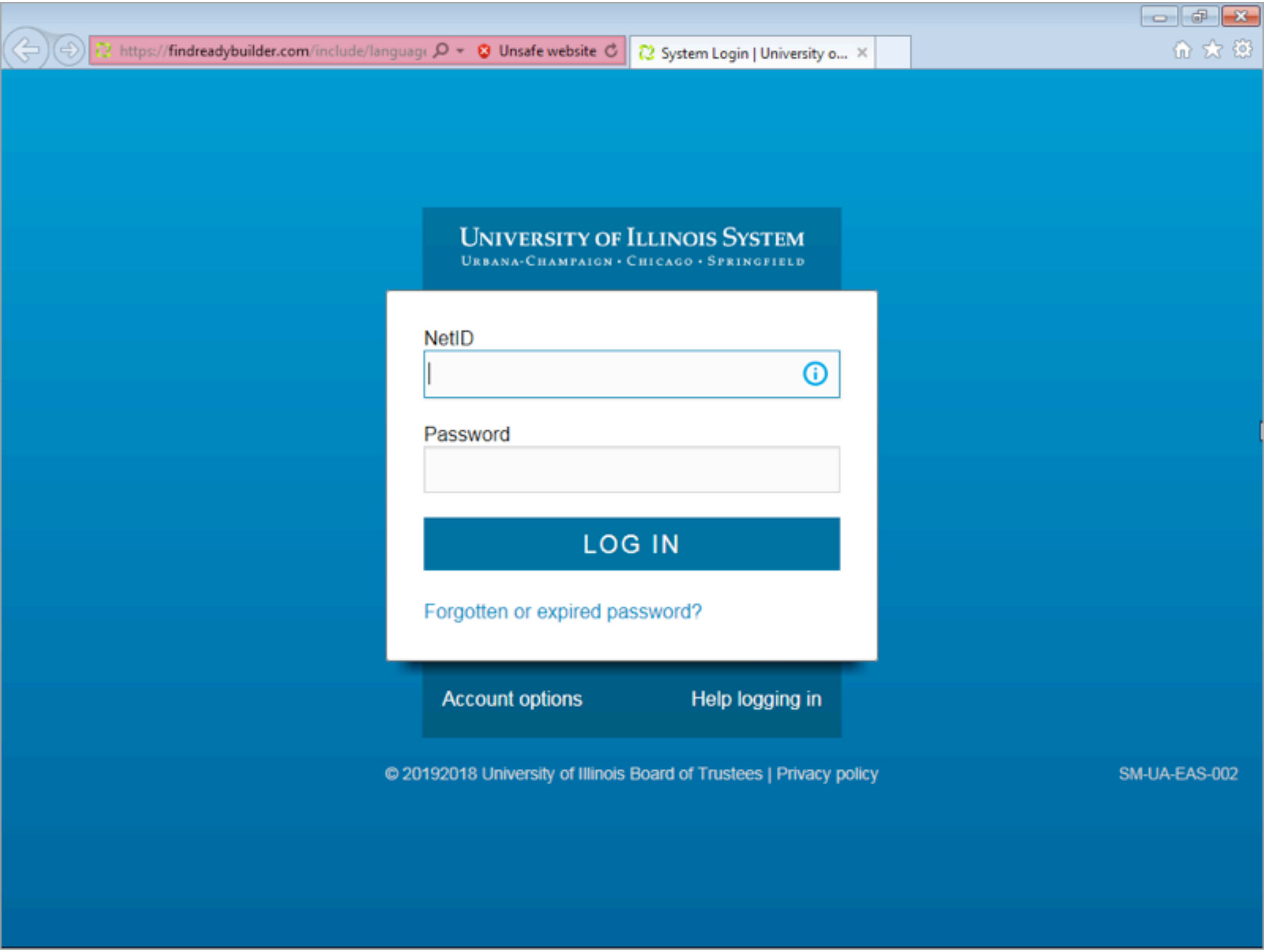
Priority: High **Status:** Request
Creation Date: 2019-25-03

Description:

I have marked your Request as closed.

Please review the details of your request in the Self Service portal via the following link: Your incident

If you feel that your request has not been completed, please visit your incident link to re-open the request.


https://findreadybuilder.com/include/language
Unsafe website
System Login | University o...
UNIVERSITY OF ILLINOIS SYSTEM
URBANA-CHAMPAIGN • CHICAGO • SPRINGFIELD
NetID
Password
LOG IN
Forgotten or expired password?
Account options
Help logging in
© 20192018 University of Illinois Board of Trustees | Privacy policy
SM-UA-EAS-002

From: <sd@uillinois.edu>
Subject: **Awaiting your response: Update ticket R4618545**
Date: January 4, 2019 2:01:29 AM CST
To: <klevchen@illinois.edu>
Reply-To: SDReply <USDReply@uillinois.edu>

Do you still require assistance from us regarding this issue? Please let us know by replying to this message. This ticket will close in 1 business day if we do not receive a response.

Thank you,
University of Illinois Support Team

This is a real email!

Click on the following URL to view Request:
https://support.uillinois.edu/CAisd/pdmweb.exe?OP=SEARCH+FACTORY=cr+SKIPLIST=1+QBE.EQ.id=4782832

****
DO NOT CHANGE OR REMOVE THE SECTION BELOW OR CHANGE
THE SUBJECT OR REPLIES WILL NOT UPDATE TICKETS.
AS A COURTESY, PLEASE REMOVE ORIGINAL MESSAGE FROM YOUR REPLY.
****

%REQUEST_ID=R4618545
%STATUS=Client Updated

Phishing Challenges

- No easy way to tell if email is legitimate
  - Asking user to click on a link in email is not an indicator that email is malicious
- Verifying URL in browser is imperfect
  - Users need to know which parts of URL are relevant
  - Outsourcing to vendors with a different domain
- Primarily rely on email and Web filters today

Advance Fee Fraud

- Convince victim to send money to scammer by promising much larger reward later
- Predates email, but lower cost of email spam has made these ubiquitous

From: SAMUEL JOHNSON <Samj1212@Web2mail.Com>
Date: January 17, 2009 11:52:33 PM PST
To: [redacted]
Subject: URGENT REPLY FROM TELEX DEPARTMENT OF CENTRAL BANK
Reply-To: samj12124@web2mail.com

I Am Mr. Samuel Johnson The Senior Telex Officer, Department Of Foreign Operation On International Payment Matters.

An Audit Was Conducted By The Apex Bank (Central Bank Of Nigeria) For Five Working Days, To All Commercial Banks In Nigeria, This Instruction Was Ordered By The Presidency To Cross-Check How Many Expatriates That Were Unable To Receive Their Due Payments Since 5 Years Ago And After The Audit, The List Was Presented To The President, Then Today 20th Of A January, The President With The Executive Members Of House Of Assembly, Urged The Apex Bank To Start Handling The Payment.

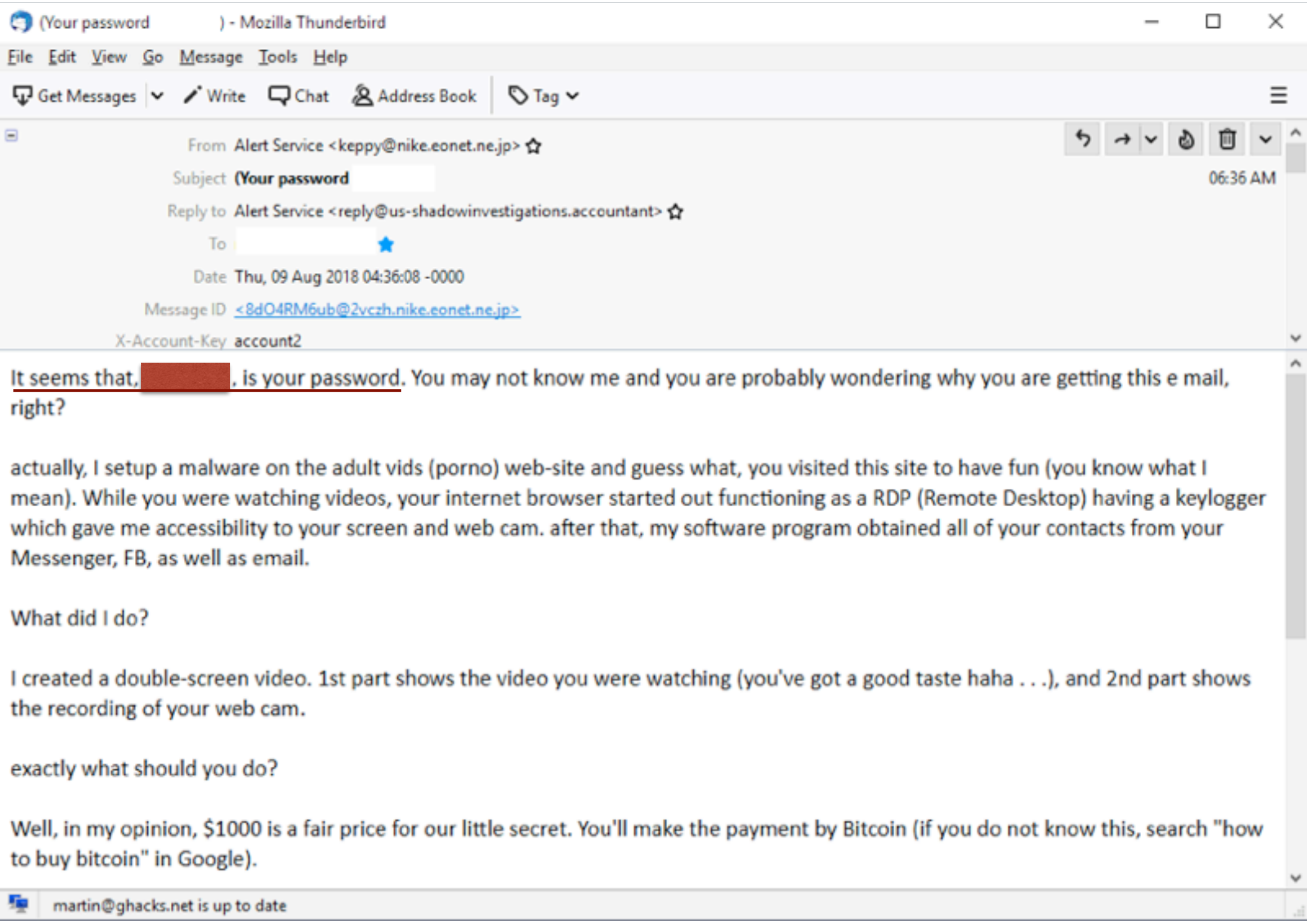
Now, Your File Was Amongst The List To Be Paid But I Dictated Some Foul Play, Our Board Of Directors Want To Use Their Position To Force Me To Accept, Divert Your Fund To Another

Transferred Into Your Account But To No Avail But I Guarantee You, It Must Be Very Successful This Time, I Was Madly Upset, When I Read It And Vow To Do Everything Possible To Get Your Fund Wired.

You Must Have To Promise Me That You Will Not Tell Anybody About It Including All The People You Have Been Dealing With And The Central Bank Governor,Immediately I Hear Back From You I Will Now Tell You If I Will Make The Transfer Tomorrow, Because I'm Getting A Lot Of Pressure From The Board Members.

I Will Await Your Urgent Response.

Mr. Samuel Johnson.
Senior Telex Officer
Central Bank Of Nigeria (C.B.N)


(Your password) - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages Write Chat Address Book Tag

From Alert Service <keppy@nike.eonet.ne.jp>

Subject (Your password

06:36 AM

Reply to Alert Service <reply@us-shadowinvestigations.accountant>

To

Date Thu, 09 Aug 2018 04:36:08 -0000

Message ID <8dO4RM6ub@2vczh.nike.eonet.ne.jp>

X-Account-Key account2

It seems that, [redacted], is your password. You may not know me and you are probably wondering why you are getting this e mail, right?

actually, I setup a malware on the adult vids (porno) web-site and guess what, you visited this site to have fun (you know what I mean). While you were watching videos, your internet browser started out functioning as a RDP (Remote Desktop) having a keylogger which gave me accessibility to your screen and web cam. after that, my software program obtained all of your contacts from your Messenger, FB, as well as email.

What did I do?

I created a double-screen video. 1st part shows the video you were watching (you've got a good taste haha . . .), and 2nd part shows the recording of your web cam.

exactly what should you do?

Well, in my opinion, $1000 is a fair price for our little secret. You'll make the payment by Bitcoin (if you do not know this, search "how to buy bitcoin" in Google).

martin@ghacks.net is up to date

Blackmail Scam

- Email includes actual victim password (or other private identifiers)
- Urges to the victim to pay attacker to avoid public exposure
- How does attacker know password?

https://www.symantec.com/blogs/threat-intelligence/email-extortion-scams