Spam

Kirill Levchenko
KLEVCHEN@CS.UCSD.EDU
What is spam?
How Email Works

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

DNS Query (Recursive)
(by Nirlog.com)

Step 1
Question: what is the IP Address of some-webserver.com?
Answer: Here is the IP Address of some-webserver.com.

Step 2
Question: where can I find the IP Address of some-webserver.com?
Answer: I don't know but .com NameSpace should have the answer.

Step 3
Non-authoritative for some-webserver.com

Step 4
Question: What is the IP Address of some-webserver.com?
Answer: Primary DNS Server of some-webserver.com knows it.

Step 5
Question: What is the IP Address of some-webserver.com?
Answer: Primary DNS Server of some-webserver.com knows it.

Step 6
Question: What is the IP Address of some-webserver.com?
Answer: Here is the IP Address of some-webserver.com.

Step 7
Answer: Here is the IP Address of some-webserver.com.

Primary DNS Server of some-webserver.com

User's PC
My IP Address

User's Primary DNS Server (Recursion Allowed)
From: TIS-PF-NISWS <TIS-PF-NISWS@uscg.mil>
Subject: 15 NOV 2011 (JDAY 319)
Date: November 15, 2011 6:53:30 AM PST
To: gps@cgls.uscg.mil
Cc: TIS-PF-NISWS <TIS-PF-NISWS@uscg.mil>

Delivered-To: klevchenko@eng.ucsd.edu
Received: by 10.231.206.203 with SMTP id fv11cs11327ibb; Tue, 15 Nov 2011 06:54:49 -0800 (PST)
Received: by 10.68.9.130 with SMTP id z2mr43604868pba.35.1321368888283; Tue, 15 Nov 2011 06:54:48 -0800 (PST)
Received: from iport-c2-out.ucsd.edu (iport-c2-out.ucsd.edu [132.239.0.119]) by mx.google.com with ESMTPS id 7si5931488pba.17.197017336; Tue, 15 Nov 2011 06:54:47 -0800 (PST) (ESMTPS)
Received: from oec-vmmx.ucsd.edu (HELO oec-vmmx03.ucsd.edu) ([132.239.8.22]) by iport-c2-out.ucsd.edu with ESMTP; 15 Nov 2011 06:54:47 -0800 (PST)
Received: from iport-c1-out.ucsd.edu (iport-c1-out.ucsd.edu [132.239.0.176]) by oec-vmmx03.ucsd.edu (Postfix) with ESMTPS id 4a06d1f91.1271847087; Tue, 15 Nov 2011 06:54:47 -0800 (PST) (ESMTPS)
Received: from osc-cgls-wb01.uscg.mil (HELO cgls.uscg.mil) ([152.121.2.24]) by smtp-mailhub-1.uscg.mil with ESMTP id 1RQKOx-00032c-I1; Tue, 15 Nov 2011 09:54:19 -0500 (EST)
Received: from smtp-mailhub-1.uscg.mil by cgls.uscg.mil with smtp (Exim 4.63) (envelope-from <gps-bounces@cgls.uscg.mil>)
Received: from [152.121.192.52] (helo=smtp-mailhub-1.uscg.mil) by cgls.uscg.mil with smtp (Exim 4.63) (envelope-from <TIS-PF-NISWS@uscg.mil>)
From: OSC-EXGW-M-001.main.ads.uscg.mil (OSC-EXGW-M-001.main.ads.uscg.mil [10.149.58.120]) by smtpout-gateway-1.uscg.mil (localhost) with ESMTP (TLS/DHE-RSA-AES256-SHA) id 388D0F1087C3884D918A640AF862FCA8E7E594@EMO-EXMB-M-103A.main.ads.uscg.mil; Tue, 15 Nov 2011 14:54:18 GMT
Authentication-Results: mx.google.com; spf=fail (google.com: domain of gps@cgls.uscg.mil does not designate 132.239.0.119 as permitted sender) client-ip=132.239.0.119; mx.google.com; spf=hardfail (google.com: domain of gps@cgls.uscg.mil does not designate 132.239.0.119 as permitted sender) smtp.mail=does not designate 132.239.0.119 as permitted sender)
Return-Path: <gps-bounces@cgls.uscg.mil>
Received-Spf: fail (google.com: domain of gps@cgls.uscg.mil does not designate 132.239.0.119 as permitted sender) client-ip=132.239.0.119; mx.google.com; spf=hardfail (google.com: domain of gps@cgls.uscg.mil does not designate 132.239.0.119 as permitted sender) smtp.mail=does not designate 132.239.0.119 as permitted sender)

Content-Class: urn:content-classes:message
Content-Type: text/plain; charset="us-ascii"

GPS Status Message Mailing List <gps.cgls.uscg.mil>

TIS-PF-NISWS@uscg.mil

GPS Status Message Mailing List <gps.cgls.uscg.mil>
GPS Status Message Mailing List <gps.cgls.uscg.mil>
list arch 2.1.13
gps@cgls.uscg.mil

http://cgls.uscg.mil/pipermail/gps
http://cgls.uscg.mil/mailman/listinfo/gps
http://cgls.uscg.mil/mailman/listinfo/gps
http://cgls.uscg.mil/mailman/options/gps

Does not designate 132.239.0.119 as permitted sender) client-ip=132.239.0.119;
from [152.121.192.52] (helo=smtp-mailhub-1.uscg.mil) by cgls.uscg.mil with smtp (Exim 4.63) (envelope-from <gps-bounces@cgls.uscg.mil>); Tue, 15 Nov 2011 09:54:19 -0500 (PST)

E=Sophos;i="4.69,515,1315206000"; d="scan'208";a="655321425"
X-Ironport-Anti-Spam-Filter: true
X-Ironport-Anti-Spam-Result: AhsHAEN8wk6E7wgW2dsb2JhbABBA6pkD4F0AQEDAQEBLQoMCAIeCwMDAQIQAwEqAgQOCAIGAQBwQgKFW
X-Ironport-Anti-Spam-Result: AuEAAEN8wk6YeQIYkbWdsb2JhbABBA6QD0EQEBLoCMcMDAQIQAwEqAgQOCAIGAQBwQgKFW
X-Ironport-Av: E=Sophos;i="4.69,515,1315206000"; d="scan'208";a="655263252"
X-Ironport-Av: E=Sophos;i="4.69,515,1315206000"; d="scan'208";a="6555263252"
X-Spam-Status: No
X-Spam-Level:  
X-Mimeole: Produced By Microsoft Exchange V6.5
Content-Class: urn:content-classes:message
Mime-Version: 1.0
Message-Id: <388D0F1087C3884D918A640AF862FCA8E7E594@EMO-EXMB-M-103A.main.ads.uscg.mil>
X-Ms-Has-Attach:
X-Ms-Tnef-Correlator: 
Thread-Topic: 15 NOV 2011 (JDAY 319)
Thread-Index: Acyjplbr6yGxWH8+Qdi+wNJ0aleEAg==
X-Proofpoint-Virus-Version: vendor=fsecure engine=2.50.10432:5.5.7110, 1.0.211, 0.0.0000 definitions=2011-11-15_02:2011-11-15, 2011-11-15,
X-Beenthere: gps@cgls.uscg.mil
X-Mailman-Version: 2.1.13
First Generation Spam

- Send spam directly to users via SMTP
- Very simple
Second Generation Spam

- Send spam via SMTP proxies
- Modify messages in minor ways
Third Generation Spam

- Send via botnet (plain SMTP)
- Modify messages more aggressively
  - Inuendo: “Excellent hardness is easy”
- Image spam
Image Spam

Xanax
Meridia
VIAGRA from $3.33 per pill
Soma
CIALIS from $3.75 per pill
Prozac
VALIUM from $1.21 per pill
Ambien
1. Compromise as many devices as possible

2. Send commands to bots

3. Execute commands
The Storm Botnet

1224739062~!vern@icir.org
ckanich@cs.ucsd.edu
savage@cs.ucsd.edu
kreibich@icir.org
...

1224720409~!eduardo
rafael
katiera
chris
johnny
...

1224739062~!vern@icir.org
From: <johnny@hotmail.com>
To: <kreibich@icir.org>
Subject: Say hello to bluepill!
spammerdomain3.com

Received: from dkjs.sgdsz ([132.233.197.74])
by dsl-189-188-79-63.prod-infinitum.com.mx
with Microsoft SMTPSVC(5.0.2195.6713);
Wed, 6 Feb 2008 16:33:44 -0800
From: <johnny@hotmail.com>
To: <kreibich@icir.org>
Subject: Say hello to bluepill!
spammerdomain3.com
Where bots come from

• **Old model:** infection campaigns
  • E.g.: Storm’s ecard campaigns

• **New model:** Pay-per-install
  • E.g. Rustock botnet
Your download will start in 5 seconds.
If your download does not start, click here

©2000-2008 FunnyPostCard.com - All rights reserved.
Installs4Sale.net - надежный сервис по загрузкам, достойный доверия

Контакты:
- 560869831
- 550525933
- info [at] installs4sale.net

Приемущества:
- Быстро осуществляем отгрузку практически в любой регион. Принимаем заказы на микусы стран по вашему выбору.
- Для постоянных клиентов действуют скидки и бонусы в виде дополнительного объема загрузок.
- Закладка по всему миру, получите несравненную прибыль, не ограничиваясь в потребностях.
Договориться по всем ценам и получить индивидуальные условия вы можете в службе поддержки. Пишите!

Мы отслеживаем уникальность инсталов и их чистоту перед продажей.

УСЛОВИЯ

Мы работаем строго по предоплате. Допускается частичная оплата постоянным клиентам на большие объемы.

Мы не несем ответственности за то что у вас по каким-то причинам отсутствуют загрузки. Если вы не видите инсталов с первых минут мы можем произошение отгрузку до выяснения обстоятельств.

ТАРИФЫ

<table>
<thead>
<tr>
<th>страна</th>
<th>цена</th>
</tr>
</thead>
<tbody>
<tr>
<td>GB (Англия)</td>
<td>150$</td>
</tr>
<tr>
<td>DE (Германия)</td>
<td>150$</td>
</tr>
<tr>
<td>USA (США)</td>
<td>130$</td>
</tr>
<tr>
<td>IT (Италия)</td>
<td>120$</td>
</tr>
<tr>
<td>Микс (US, CA, AU, GB)</td>
<td>100$</td>
</tr>
<tr>
<td>CA (Канада)</td>
<td>100$</td>
</tr>
<tr>
<td>Микс (Европа)</td>
<td>40$</td>
</tr>
<tr>
<td>Азия</td>
<td>10$</td>
</tr>
</tbody>
</table>

Все цены указаны за 1000 уникальных загрузок.
Fourth Generation Spam

- Send via botnet (Web mail)
- Send via botnet (authenticated SMTP)
- Simple messages
CAPTCHAs
Stay signed in

Enable Web History Learn More

Security question: Choose a question ...
If you forget your password we will ask for the answer to your security question. Learn More

Answer:

Recovery email:
This address is used to authenticate your account should you ever encounter problems or forget your password. If you do not have another email address, you may leave this field blank. Learn More

Location: United States

Birthday: MM/DD/YYYY (e.g. "10/30/2011")

Word Verification: Type the characters you see in the picture below.

Letters are not case-sensitive

Terms of Service: Please check the Google Account information you've entered above (feel free to change anything you like), and review the Terms of Service below.

With Gmail, you won't see blinking banner ads. Instead, we display ads you might find useful that are relevant to the context of your messages. Learn more...
CAPTCHA: Using Hard AI Problems For Security

Luis von Ahn¹, Manuel Blum¹, Nicholas J. Hopper¹, and John Langford²

A CAPTCHA is a program that can generate and grade tests that: (A) most humans can pass, but (B) current computer programs can’t pass. Such a program can be used to differentiate humans from computers and has many applications for practical security, including (but not limited to):

Free Email Services. Several companies (Yahoo!, Microsoft, etc.) offer free email services, most of which suffer from a specific type of attack: “bots” that sign up for thousands of email accounts every minute. This situation can be improved by requiring users to prove they are human before they can get a free email account. Yahoo!, for instance, uses a CAPTCHA of our design to prevent bots from registering for accounts. Their CAPTCHA asks users to read a distorted word such as the one shown below (current computer programs are not as good as humans at reading distorted text).

1. Introduction
CAPTCHA Economics

- Designed to prevent automated service abuse
- Created a market for CAPTCHA-solving services
- Evolved into a mature industry
  - Very easy early CAPTCHAs attacked with OCR software
  - Today’s harder CAPTCHAs solved by people

Price of solving 1,000 CAPTCHAAs?

CAPTCHA Economics

- Simple HTTP POST API for service
  - Response time and accuracy on par with normal users
- Automation possible, but must be tuned to each type
  - Fragile, easy to break by making small change to CAPTCHA
  - Human solvers more versatile, low capital investment
- China and India dominate labor force

CAPTCHA Economics

❖ Are CAPTCHAAs a success or a failure?
❖ As a hard AI problem: (qualified) success
❖ As an absolute security mechanism: failure
❖ As an economic impediment: success

Spam pipeline

<table>
<thead>
<tr>
<th>Sent</th>
<th>MTA</th>
<th>Inbox</th>
<th>Visits</th>
<th>Conversions</th>
</tr>
</thead>
<tbody>
<tr>
<td>347.5M</td>
<td>82.7M (24%)</td>
<td></td>
<td>10,522 (0.003%)</td>
<td>28 (0.000008%)</td>
</tr>
<tr>
<td>83.6 M</td>
<td>21.1M (25%)</td>
<td>-----</td>
<td>3,827 (0.005%)</td>
<td>316 (0.00037%)</td>
</tr>
<tr>
<td>40.1 M</td>
<td>10.1M (25%)</td>
<td>---</td>
<td>2,721 (0.005%)</td>
<td>225 (0.00056%)</td>
</tr>
</tbody>
</table>

Pharma: 12 M spam emails for one “purchase”

E-card: 1 in 10 visitors execute a suggested binary
DNS Server
Only servers with a registered IP Address of 80.102.92.11 are authorised senders for the domain "@domain.uk"

Senders Domain and IP Address are checked

SMTP

Email Dropped

Copyright 2001-2007 © Gunter Ollmann