Spam | Malware

INGI2347: COMPUTER SYSTEM SECURITY (Spring 2014)

Marco Canini

UCL Université catholique de Louvain

Lecture slides adapted from UCL INGI2347 by Gildas Avoine and Upenn CSE331 by Steve Zdancewic

Announcements

- There is no class on 3 Feb
- First challenge announced on 4 Feb

Plan for today

Lecture 2

- Spam
  - Introduction
  - Techniques
  - Protection
- Malware
  - Malicious code
  - Web exploits
  - Buffer overflow

Introduction to Spam

Email spam

Typically defined as

- Unsolicited automated email
- Sent in bulk to numerous recipients
- (The sender is a stranger to the recipient)

Why is it a problem?

- Lost productivity
  - Symantec: Study on 1000 users shows 65% spend more than 10’ a day to delete spam emails, 24% more than 20’
- Stress on the infrastructure
  - Sophos: “92.3 percent of all email sent during the first three months of 2008 was spam”
- Annoying
  - Useful emails lost

The 10 Worst Spam Countries

1	**United States**	Number of Current Live Spam Issues: 2953
2	**China**	Number of Current Live Spam Issues: 1196
3	**Russian Federation**	Number of Current Live Spam Issues: 754
4	**Ukraine**	Number of Current Live Spam Issues: 549
5	**Japan**	Number of Current Live Spam Issues: 437
6	**United Kingdom**	Number of Current Live Spam Issues: 404
7	**Brazil**	Number of Current Live Spam Issues: 352
8	**India**	Number of Current Live Spam Issues: 316
9	**Germany**	Number of Current Live Spam Issues: 311
10	**France**	Number of Current Live Spam Issues: 296

Source: Spamhaus Blocklist (BSL) database http://www.spamhaus.org/statistics/countries/

Most common products advertised

Pharmacy	81%
Replica	5.40%
Enhancers	2.30%
Phishing	2.30%
Degrees	1.30%
Casino	1.00%
Weight Loss	0.40%
Other	6.30%

Source: Commtouch Software Ltd., 2010

Fw: Hey there - Liable Medicinal Store, best chance to save http://berkatmotor.com

Re: Hey there - Superior Drugs Online Website, save and reserve money http://gzn

Fw: Hello there - Your World Class Medicinal Web store, try our amount saving htt

Deutsche Top-Online Casinos - Auf unseren Webseiten finden Sie die besten Onl

Fw: Hey - The Liable Pharma Online Products, visit and save up your money now h

INVESTMENT INTEREST. - Greetings, I am representing an investment interest fr

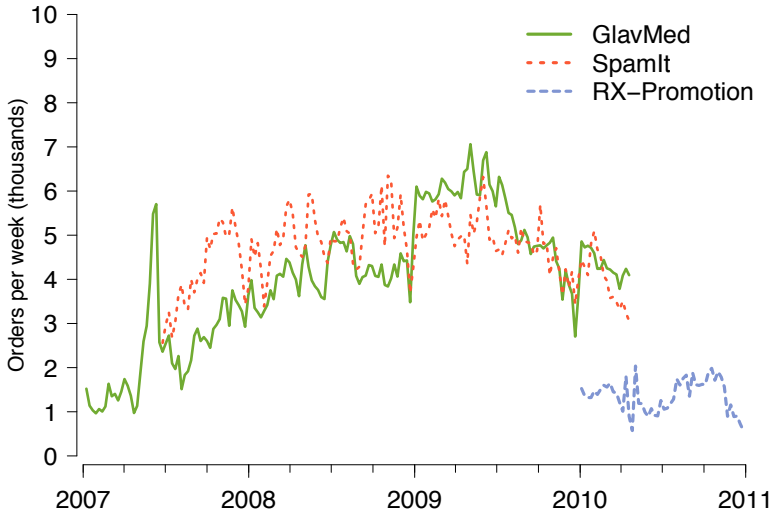
Hello there - Your Accessible Pharma Online Supplies, knock-down price http://ww

Hello there - The Superb Medic Online Store, visit and save http://sixstone.pronet.

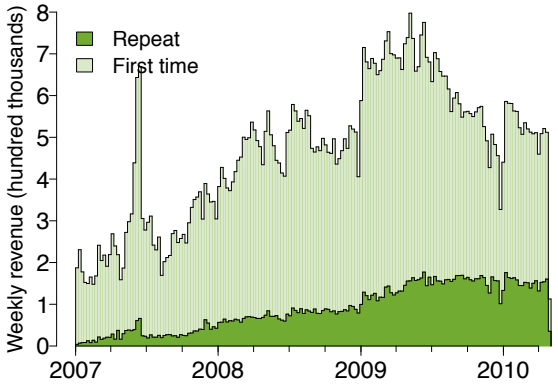
RE: Hello there - The Liable Medicines Products, time for financial saving http://ba

Business of Online Pharmaceutical Affiliate Programs

Weekly sales volume for each of the programs.



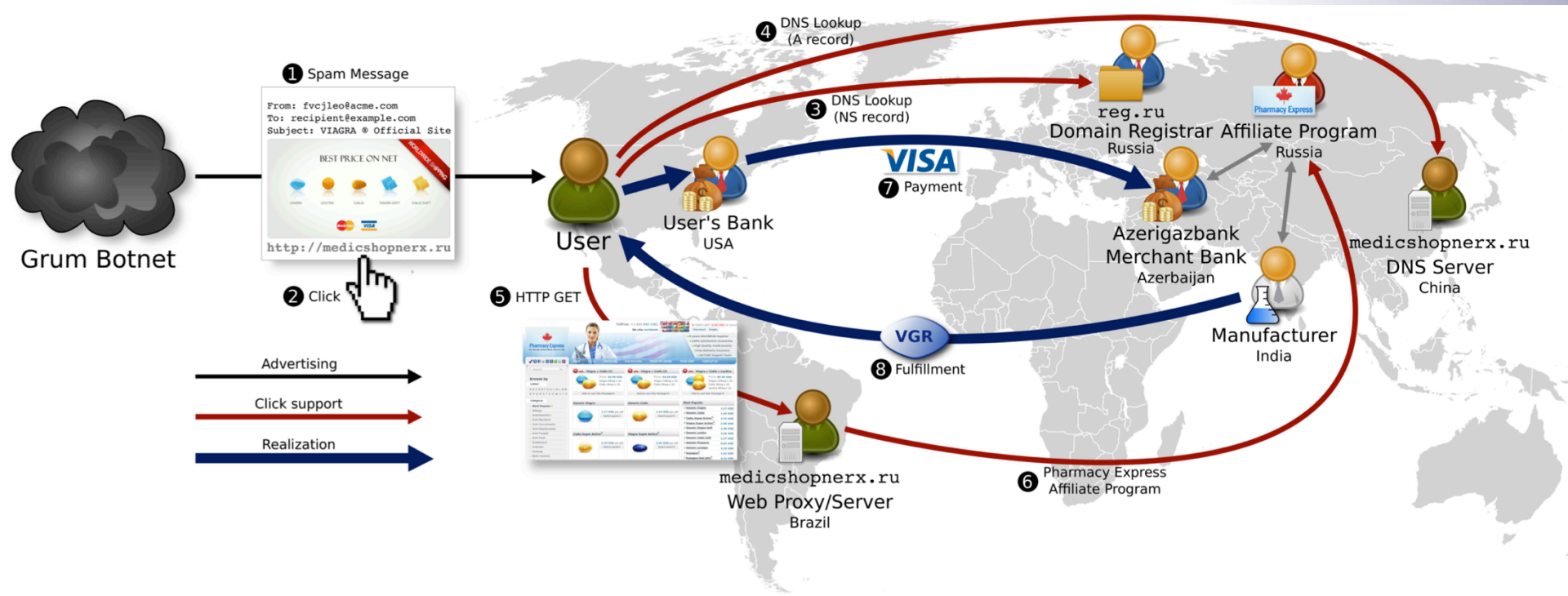
Weekly order revenue shown by customer class.



(a) GlavMed

Source: McCoy et al., PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs, 2012

Infrastructure involved in a single URL's value chain



Source: Levchenko et al., Click Trajectories: End-to-End Analysis of the Spam Value Chain, 2011

Spamming Techniques

Spamming Techniques

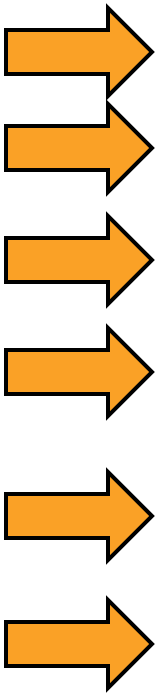
- The sender address is (almost) always forged to prevent counterattacks

- Method 1: Use of own/ISP SMTP server

SMTP

- The protocol used by mail servers on the Internet is SMTP (Simple Mail Transfer Protocol)
  - RFC 821, 1982
- SMTP uses TCP connections on port 25
- It knows a few simple commands such as:
  - HELO (announces a server)
  - MAIL FROM: (defines sender)
  - RCPT TO: (defines destination)
  - DATA: (defines content)

SMTP example



```
bash$ telnet smtp.sgsi.ucl.ac.be 25
Trying 2001:6a8:3080:9:2::67...
Connected to smtp.sgsi.ucl.ac.be (2001:6a8:3080:9:2::67).
Escape character is '^]'.
220 smtp5.sgsi.ucl.ac.be ESMTP
HELO smtp.sgsi.ucl.ac.be
250 smtp5.sgsi.ucl.ac.be
MAIL FROM: this-can-be@anythi.ng
250 2.1.0 Ok
RCPT TO: marco.canini@uclouvain.be
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Hi
.
250 2.0.0 Ok: queued as 1A000198046
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```

Mail Path

- The message is accepted by and stored in an SMTP server
- That server will send it to another server closer to the destination
- At its destination it will be delivered in the recipient's mailbox

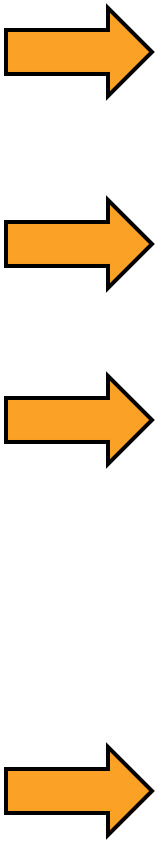
Forged Emails

- As Basic SMTP does not perform any verification of the sender's address, it is easy to forge mails
- Mainly used for:
  - Spamming, phishing, propagating rumors
- Each server adds a header to the mail

Limitation: originating system can be traced

- The server that receives the mail initially notes:
  - The contents of the HELO command
  - The IP address of the mail's sender
  - The receiving time
- With these data, it is possible to trace the originating system
- Often easy to find the author of the mail
  - Author can be identified by the system log
- Much harder if the system doesn't log users

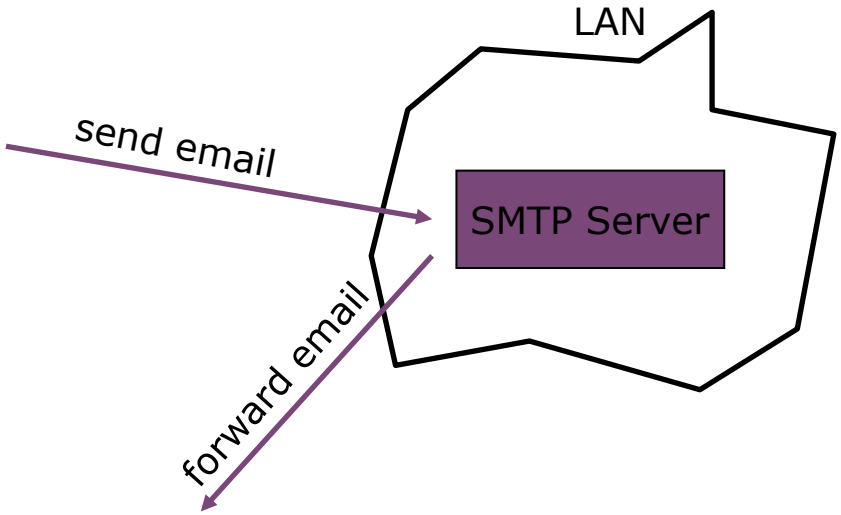
Tracking



```
Delivered-To: m.canini.c@ieee.org
Received: from smtp6.sgsi.ucl.ac.be (smtp.sgsi.ucl.ac.be. [130.104.5.67])
        by mx.google.com with ESMTP id fo15si7407415wic.42.2014.01.27.16.06.45
        for <m.canini.c@ieee.org>;
        Mon, 27 Jan 2014 16:06:45 -0800 (PST)
Received: from mmp-1-1.sipr-dc.ucl.ac.be (mmp-1-1.sipr-dc.ucl.ac.be [10.1.3.4])
         by smtp6.sgsi.ucl.ac.be (Postfix) with ESMTP id 455901C6ADF
         for <m.canini.c@ieee.org>; Tue, 28 Jan 2014 01:06:38 +0100 (CET)
Received: from smtp5.sgsi.ucl.ac.be (unknown [10.1.5.5])
 by mmp.sipr-dc.ucl.ac.be
 (Oracle Communications Messaging Exchange Server 7u4-19.01 64bit (built Sep  7
 2010)) with ESMTP id <0N0300IT74B2I8A0@mmp.sipr-dc.ucl.ac.be> for
 m.canini.c@ieee.org (ORCPT marco.canini@uclouvain.be); Tue,
 28 Jan 2014 01:06:38 +0100 (CET)
From: this-can-be@anythi.ng
Received: from smtp.sgsi.ucl.ac.be (haproxy2.sipr.ucl.ac.be [130.104.5.120])
         by smtp5.sgsi.ucl.ac.be (Postfix) with SMTP id 1A000198046 for
 <marco.canini@uclouvain.be>; Tue, 28 Jan 2014 01:06:31 +0100 (CET)
```

Spamming Techniques (Cont')

- Method 2: Abuse of open relays
  - A single message is dropped into a few SMTP servers with thousands of destination addresses each
  - The abused servers politely send out one copy of the message to each destination



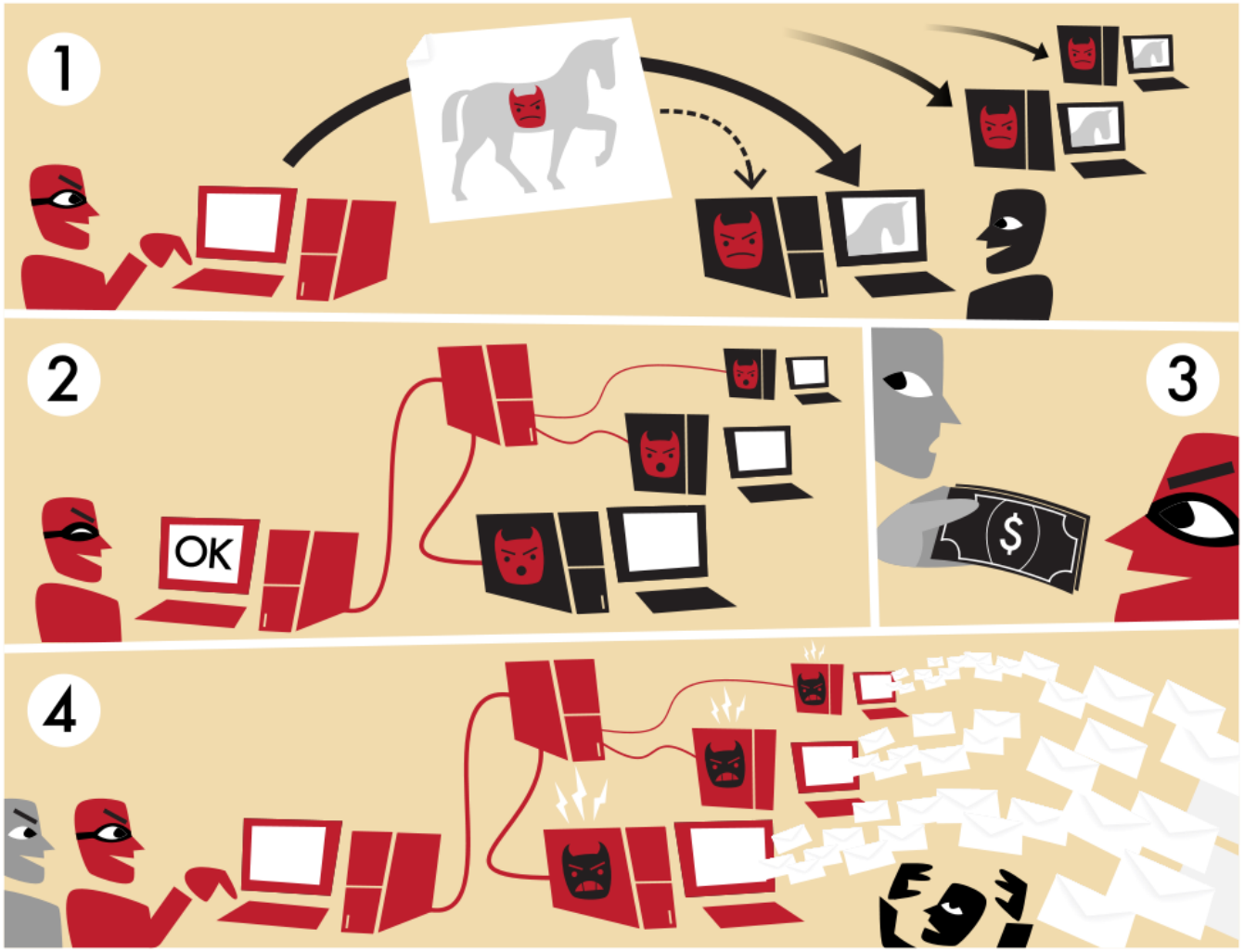
Limitation: servers do not operate as open relays

- For a message to be accepted by the mail server, either the sender's or the recipient's address has to belong to the same domain as the server
- Only systems belonging to the same domain as the mail server can send messages, with the sender being a part of the domain
- An open relay used for SPAM will be detected and included into a blacklist, to be avoided by other servers

Spamming Techniques (Cont')

- Method 3: abuse a webmail account
  - Use a script to open many webmail accounts
  - Send spam until accounts are closed
- Method 4: hack into home computers
  - Use a virus that infects home computers (turning them into "bots")
  - Use a network of bots to send out spam

How it works



Source: Wikipedia

The typical affiliate earns about $100 per 1,000 infected hosts

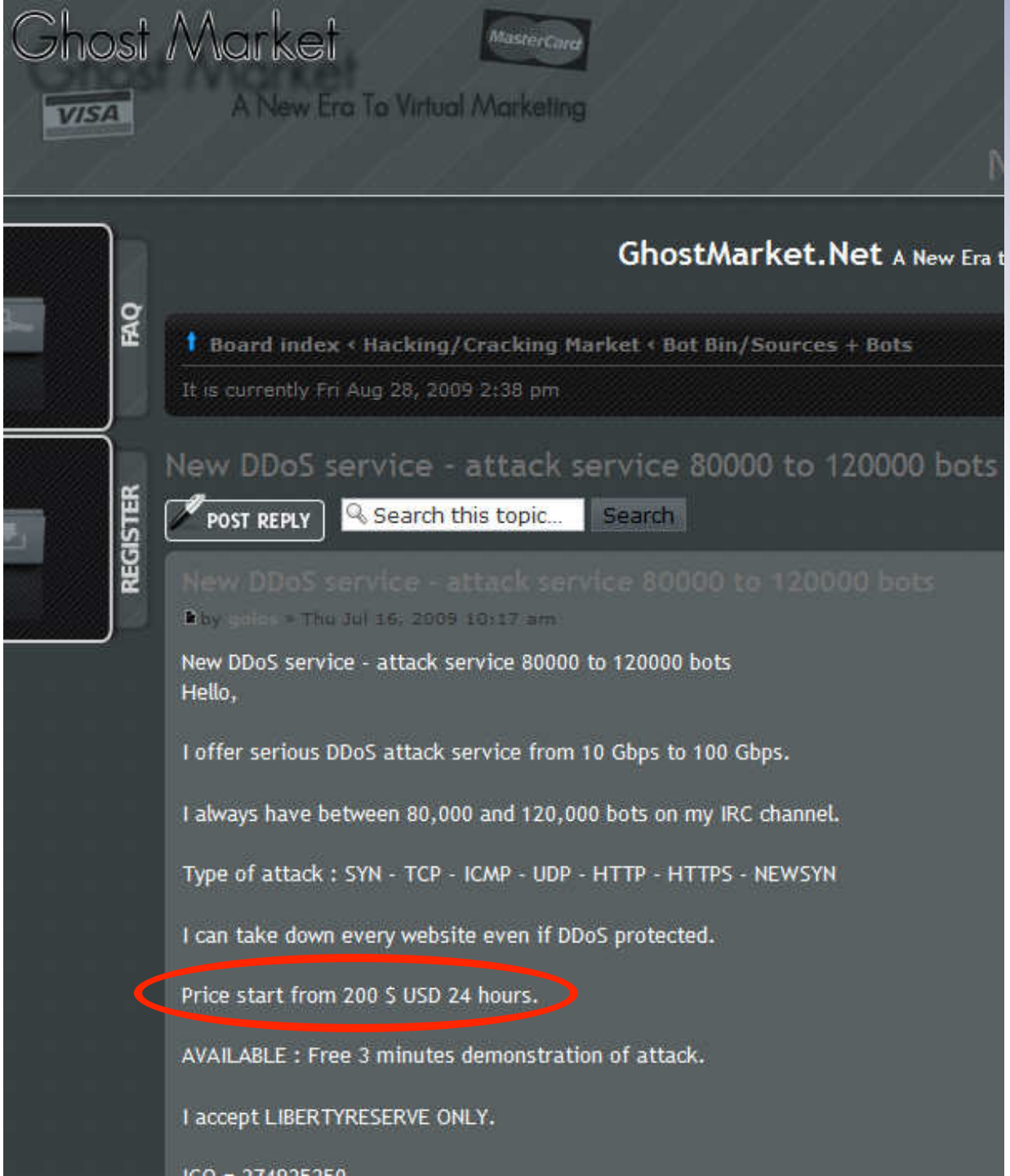
Botnets (illegal)

- A collection of machines infected with a malicious program – the bot – and controlled by a third party (hacker)
- Bots connect to a command and control (C&C) server
  - Often an Internet Relay Chat (IRC) server
  - But in some cases a web server or P2P network to avoid detection
- Botnets are rented for cheap
  - 1,000 US-based hosts $200
  - 1,000 EU-based hosts $60-$120
  - 1,000 international mix type of hosts is $20

Botnets for Sale

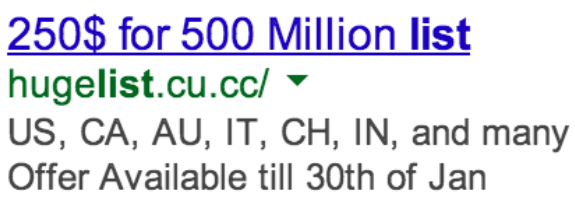
Not just spam:

- DDoS
- Click fraud
- Forum spam posts



How do spammers harvest email addresses?

- Just buy an email list
- Crawl the Web



- Mailing lists & newsgroups
- By guessing (dictionary, brute force, standard)
  - Confirm valid addresses:
    - Wait for an error message
    - Use 'Return-Receipt-To' header or send HTML message with a ref. to an external image
- Hack into a database
- Scan files on infected machines
- Hoax, scam and chain letters

Hoax example

Subject: Dear Respected One,

Dear Respected One,
GREETINGS,

Permit me to inform you of my desire of going into business relationship with you. I got your contact from the International web site directory. I prayed over it and selected your name among other names due to it's esteeming nature and the recommendations given to me as a reputable and trust worthy person I can do business with and by the recommendations I must not hesitate to confide in you for this simple and sincere business.

I am Wumi Abdul; the only Daughter of late Mr and Mrs George Abdul. My father was a very wealthy cocoa merchant in Abidjan,the economic capital of Ivory Coast before he was poisoned to death by his business associates on one of their outing to discus on a business deal. When my mother died on the 21st October 1984, my father took me and my younger brother HASSAN special because we are motherless. Before the death of my father on 30th June 2002 in a private hospital here in Abidjan. He secretly called me on his bedside and told me that he has a sum of $12.500.000 (Twelve Million, five hundred thousand dollars) left in a suspense account in a local Bank here in Abidjan, that he used my name as his first Daughter for the next of kin in deposit of the fund.

He also explained to me that it was because of this wealth and some huge amount of money his business associates supposed to balance his from the deal they had that he was poisoned by his business associates, that I should seek for a God fearing foreign partner in a country of my choice where I will transfer this money and use it for investment purpose, (such as real estate management). Sir, we are honourably seeking your assistance in the following ways.

1) To provide a Bank account where this money would be transferred to.
2) To serve as the guardian of this since I am a girl of 26 years.

Moreover Sir, we are willing to offer you 15% of the sum as compensation for effort input after the successful transfer of this fund to your designate account overseas. please feel free to contact ,me via this email address
wumi1000abdul@yahoo.com

Anticipating to hear from you soon.
Thanks and God Bless.
Best regards.
Miss Wumi Abdul

PLEASE FOR PRIVATE AND SECURITY REASONS,REPLY ME VIA EMAIL:
wumi1000abdul@yahoo.com

Fighting spam

Stopping spam

- Anti-spam laws
  - Legislation to restrict use of email spam in several countries
    - "Legal definitions of spam, influenced presumably by lobbyists, tend to exclude mail sent by companies that have an "existing relationship" with the recipient. But buying something from a company, for example, does not imply that you have solicited ongoing email from them" – Paul Graham
- Protection via a technical solution
  - Filters
    - "I think it's possible to stop spam, and that content-based filters are the way to do it. The Achilles heel of the spammers is their message. They can circumvent any other barrier you set up. They have so far, at least. But they have to deliver their message, whatever it is. If we can write software that recognizes their messages, there is no way they can get around that" – Paul Graham, 2002
  - Black/white/grey lists

Filters

- Feature-recognizing filters
  - Rules that recognize individual properties of spam
    - E.g. mentions "Viagra", has all uppercase subject, etc.
  - Assign a spam "score" to email
  - How many points should an email get for having the word "drug" in it?
- Statistical filtering based on the Bayesian approach
  - Proposed by Paul Graham in 2002 (http://www.paulgraham.com/spam.html)
  - Trained on user's email labeled as spam vs. not spam
  - Assigns each message with a probability of being spam
- Filters are not perfect and can not prevent false positives or false negatives

SpamAssassin

- One of the most effective spam filters
- Open Source
- Rules use positive/negative score
- Several hundred rules
  - http://spamassassin.apache.org/tests_3_3_x.html
- Reinforce its own rules through Bayesian filtering

Rule example

Talks about an E.D. drug using its chemical name	DRUG_ED_SILD
Mentions Generic Viagra	DRUG_ED_GENERIC
Fast Viagra Delivery	DRUG_ED_ONLINE
Online Pharmacy	ONLINE_PHARMACY
No prescription needed	NO_PRESCRIPTION
Attempts to disguise the word 'viagra'	VIA_GAP_GRA
Two or more drugs crammed together into one word	DRUGS_SMEAR1
Relay HELO'd with suspicious hostname (mail.com)	FAKE_HELO_MAIL_COM_DOM
Relay HELO'd using suspicious hostname (Rogers)	HELO_DYNAMIC_ROGERS
Relay HELO'd using suspicious hostname (T-Dialin)	HELO_DYNAMIC_DIALIN

Black lists

- E.g. Spamhaus SBL and XBL lists
  - http://www.spamhaus.org/
  - SBL: IPs of known spam operators
  - XBL: IPs of hijacked systems relying spams
- Mail servers can use this database to decide the acceptance of electronic mail

Policy Block List

- Database of end-user IP address ranges which should not be delivering unauthenticated SMTP email to any Internet mail server except those provided for specifically by an ISP for that customer's use
- Pros:
  - Cheap
  - Easy to put into practice
- Cons:
  - Centralized and always up to date list to be effective
  - Many false negative

White lists

- Instead of blocking some emails, the reception is allowed only if the sender (domain, IP address, etc.) belongs to the white list
- Pros:
  - Cheap
  - Easy to put into practice
- Cons:
  - Authorized senders must be known *a priori*
  - Many false positive

Spam database

- Database maintained on a centralized server
- Check whether the received message appears in the database
- Pros:
  - The database is shared
  - Few false positive
- Cons:
  - Do not detect variant of spam
  - Require computation and bandwidth
  - Many false negative

Greylisting

- Basic idea: block a mail if the behavior of the sender's server is abnormal
- The recipient server manages a database that contains "triplet" for each incoming mail:
  - The IP address of the connecting host
  - The sender address
  - The recipient address
- The database is a kind of white list

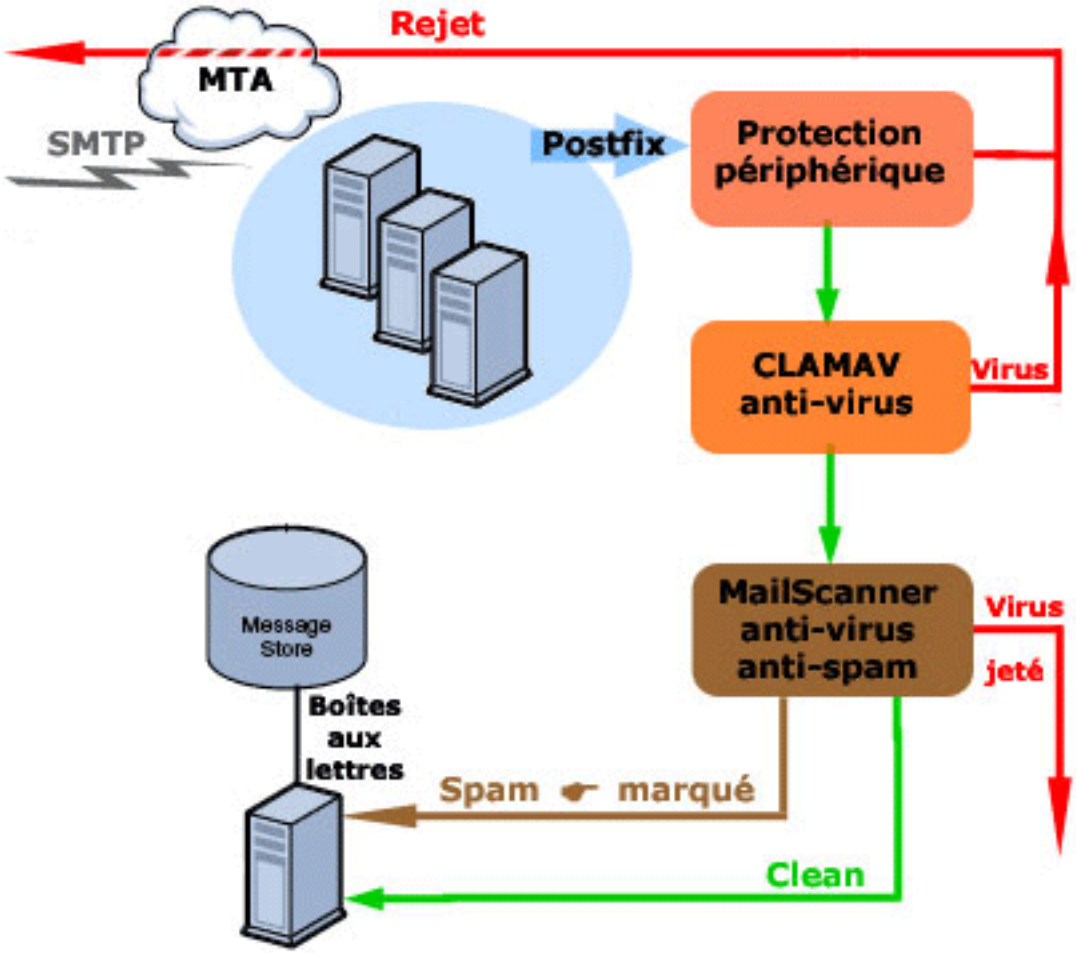
Greylisting

- When the server receives a mail, it checks whether it already belongs to the database
  - If not, the mail is greylisted for a short time and an error message is returned to the sender server
  - If the sender server is compliant with RFC2821, it should retry the transmission after at least 30 minutes
  - The greylisted mail is then unblocked
- Pros:
  - No or few false negative
- Cons:
  - Delays due to the greylisting

Alternative solutions ?

- Registered computers/users
  - Designate the machines allowed to send e-mail with a sender address originating in the domain
    - One standard is Sender Policy Framework (SPF)
- Challenge/response
  - User must answer to a challenge to be added to the white list
- Adding cost to emails
  - Computer must carry out computation to send an email
- Delegate: use gmail

At UCL



Source: http://www.uclouvain.be/12703.html | More: http://www.uclouvain.be/7489.html

Plan for today

Lecture 2

- Spam
  - Introduction
  - Techniques
  - Protection
- Malware
  - Malicious code
  - Web exploits
  - Buffer overflow

Malware

Malicious code or Malware

- Viruses
- Worms
- Trojan horses
- Backdoors
- Rootkit
- Spyware
- Adware

Malicious code or Malware

- Viruses – propagates with help of other programs
- Worms – self-contained programs
- Trojan horses – pretends to do one thing; does another
- Backdoors – secret entry point into a system
- Rootkit – hides the presence of other malware
- Spyware – sends personal information to third party
- Adware – shows Ads

Effects of Malware

- Data loss
- Denial of Service
  - Crash machines / Functional loss / Overload network infrastructure
  - Loss of productivity
- Creates “bots” to attack other systems
- Loss of confidentiality
  - E.g. SirCam sends a random file on the disk to contacts
  - E.g. Bugbear sends the password stored by IE

Viruses & Worms

- A computer virus/work is a (malicious) program
  - Creates (possibly modified) copies of itself
  - Often has other effects (deleting files, "jokes", messages)
- Viruses cannot propagate without a "host"
  - Typically require some user action to activate
- Worms are self-contained running programs
  - Infection strategy more active
  - Exploit vulnerabilities to propagate itself

Virus/Worm Writer's Goals

- Hard to detect
- Hard to destroy or deactivate
- Spreads infection widely/quickly
- Can reinfect a host
- Easy to create
- Machine/OS independent

Virus Evolution

Classical period

- Passive propagation through floppy disks exchange
- Slow propagation and hence need to be efficient
- First known virus (Apple II): Elk Cloner created in 1982 by Rich Skrenta, a 15-year-old high school student
  - It was a joke, simply showed a poem
- First PC virus: Brain, spread in 1986
  - Displayed the address of the authors when computer booted, and replaced the disk label by @brain

Virus Evolution

Modern period

- Viruses/worms use Internet to actively propagate
- They can infect the planet in a few hours
- Real threat as they propagate much faster than the anti-virus software can be updated

Kind of Viruses

- Boot sector viruses
  - Historically important, but less common today
- Memory resident viruses
  - Standard infected executable
- Macro viruses
  - Embedded in documents (e.g. Word docs)
  - Macros are programs in a scripting language (e.g. Visual Basic Script)

Stealth Viruses

- Simple: the virus compresses the original file, and creates an infected file of the same size
- Complex: the virus modifies the system so as to become invisible
  - E.g. modifies file reading routines so that they don't reveal the virus
- Examples:
  - Brain (1986): infects the boot sector but keeps an original copy. It redirects all access to the boot sector towards the copy.

Polymorphic Viruses

Malicious code is effectively detected with signatures

- Polymorphic viruses mutate themselves during replication so as to remain undetectable
  - Encrypt most of the virus with a different random key each time
    - Virus decrypts main body using random key
    - Jumps to the code it decrypted
    - When replicating, generate a new key and encrypt the main part of the replica
  - To avoid signature-based detection the remaining code must be modified while keeping the same functionality
    - Insert no-op instructions: subtract 0, move value to itself
    - Reordering independent instructions
    - Using equivalent instruction sequences

Strategies for Polymorphic Viruses

- Encrypt most of the virus with a different random key each time
  - Virus decrypts main body using random key
  - Jumps to the code it decrypted
  - When replicating, generate a new key and encrypt the main part of the replica

Melissa Macro Virus

- First instantaneous planetary virus, discovered on 26 Mar, 1999
- Although not originally designed for harm, Melissa shut down Internet email systems that got clogged with infected emails propagating from the virus
- A Word document received by email containing Visual Basic Script code associated with the "document.open" method of Word
- Send email message to the first 50 addresses in the address book
- The author David L. Smith was arrested within a week and sentenced to 20 months and fined $5,000

Love Letter Worm, aka «ILOVEYOU»

- Arrived as email with a Visual Basic Script attachment
- Exploited Window's extension hiding to display a fake "txt" extension for the original file iloveyou.txt.vbs
- Propagates by email to all addresses in the address book
- Also propagates through IRC
- Modifies IE's home page
- Replaces several different kinds of files with copies of itself
- ILOVEYOU caused $10 billion in damages [Landler]

ILOVEYOU Impact

American parliament science committee:

- "In one day's time, roughly 47 million people received the e-mail worldwide and the virus looked for love in all the wrong places in over 10 million computers. [...] Insurance giant Lloyd's of London has estimated the virus will cost over $15 billion in damages and lost productivity"

Backdoors

- Program that allows remote access to a system, without the user knowing about it
- Installed by Trojan horses and hence often classified as such
- Characteristics:
  - Size: small is beautiful and easier to install
  - Functionalities: downloading other programs, spying on the network, screen, keyboard
  - Communication mode: listen on predefine TCP or UDP port
  - Better: connect to a master through IRC or P2P network
  - Even better: communication via ICMP or DNS, encryption

Spywares & Adwares

- Spywares & Adwares are either installed by viruses or web pages that manipulate unpatched browsers
- They modify the browser's behavior
  - Display pop-ups with ads
  - Modify search results
  - Modify the ads that are shown in web pages
  - Change the home page
  - Collect and send private information

Rootkits

- Rootkits modify the operating system in order to hide running programs, files or configurations
  - Sony has distributed a copy protection software (XCP) that used a rootkit to prevent users to uninstall it
    - They had to offer exchange of all CDs

Exploits on the Web

Exploits

- Most software contain flaws
- These bugs can be exploited by hackers
- An exploit is a method or script that allows exploiting bugs
- The most interesting are exploits on servers
  - They can be done remotely
  - Servers often have higher privileges

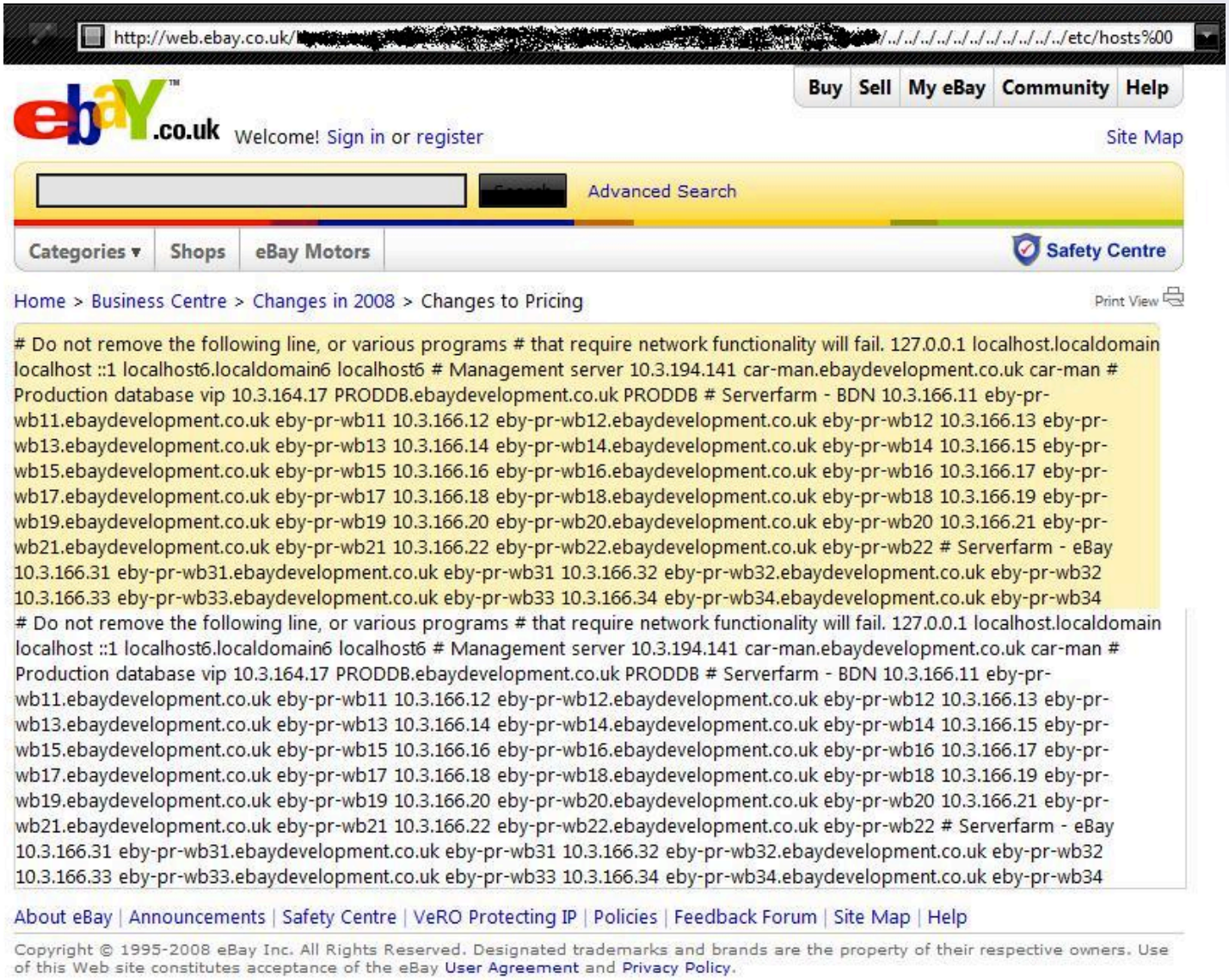
Summary of Exploits on the Web

- Directory Traversal
- Cross-Site Scripting
- Phishing
- SQL Injection

Directory Traversal

- Web server's documents are accessible from a root path
- If the server does not verify the URLs, we can access other files
- Classical example: directory traversal
  - **../../../../**
  - Weak scripts
- Easy to find
  - Google: directory traversal

Directory Traversal Example



Avoiding Directory Traversal

- Some web app. check the string .. and ../ and ../ in the URL
- However, these applications are still vulnerable to "percent encoded" URLs:
  - %2e%2e/ which is to ../
  - ..%2f which is to ../
  - %2e%2e%2f which is to ../
  - %2e%2e%5c which is to ..\
  - Etc.
- But also UTF8 encoding, etc.
- Security of the application depends on the encoding allowed by the web server

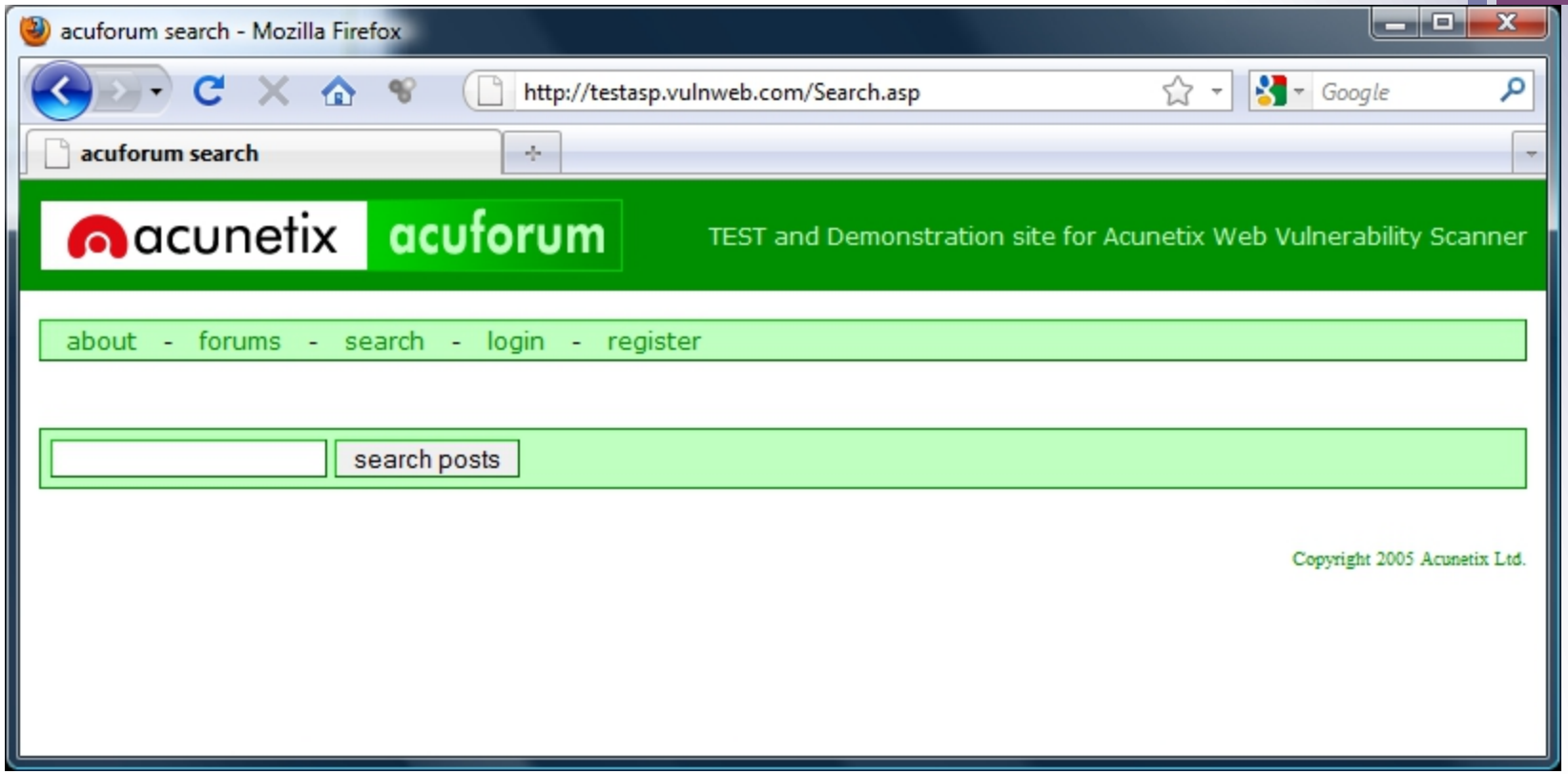
Avoiding Directory Traversal

- Open Web Application Security Project (OWASP)
  - http://www.owasp.org/index.php/Testing_for_Path_Traversal

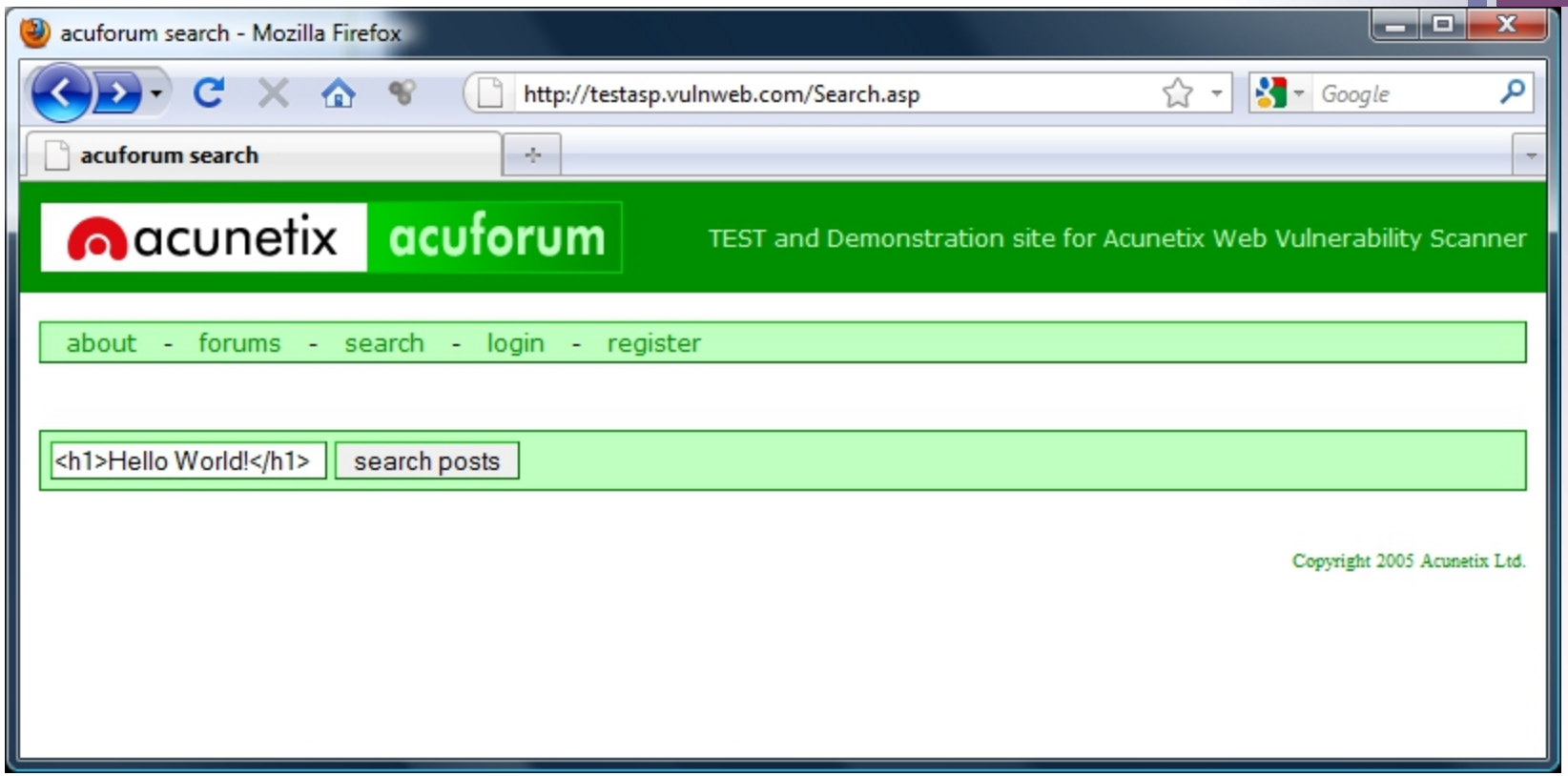
Abusing Web Applications

- Interactive web sites (e-commerce, e-banking, etc.) are created with scripts
- Forms are written in HTML
- The client fills them up and clicks on a button
- The button generates a request containing all the parameters of the form
- The request calls a script that performs an operation with the parameters and returns a web page as a result

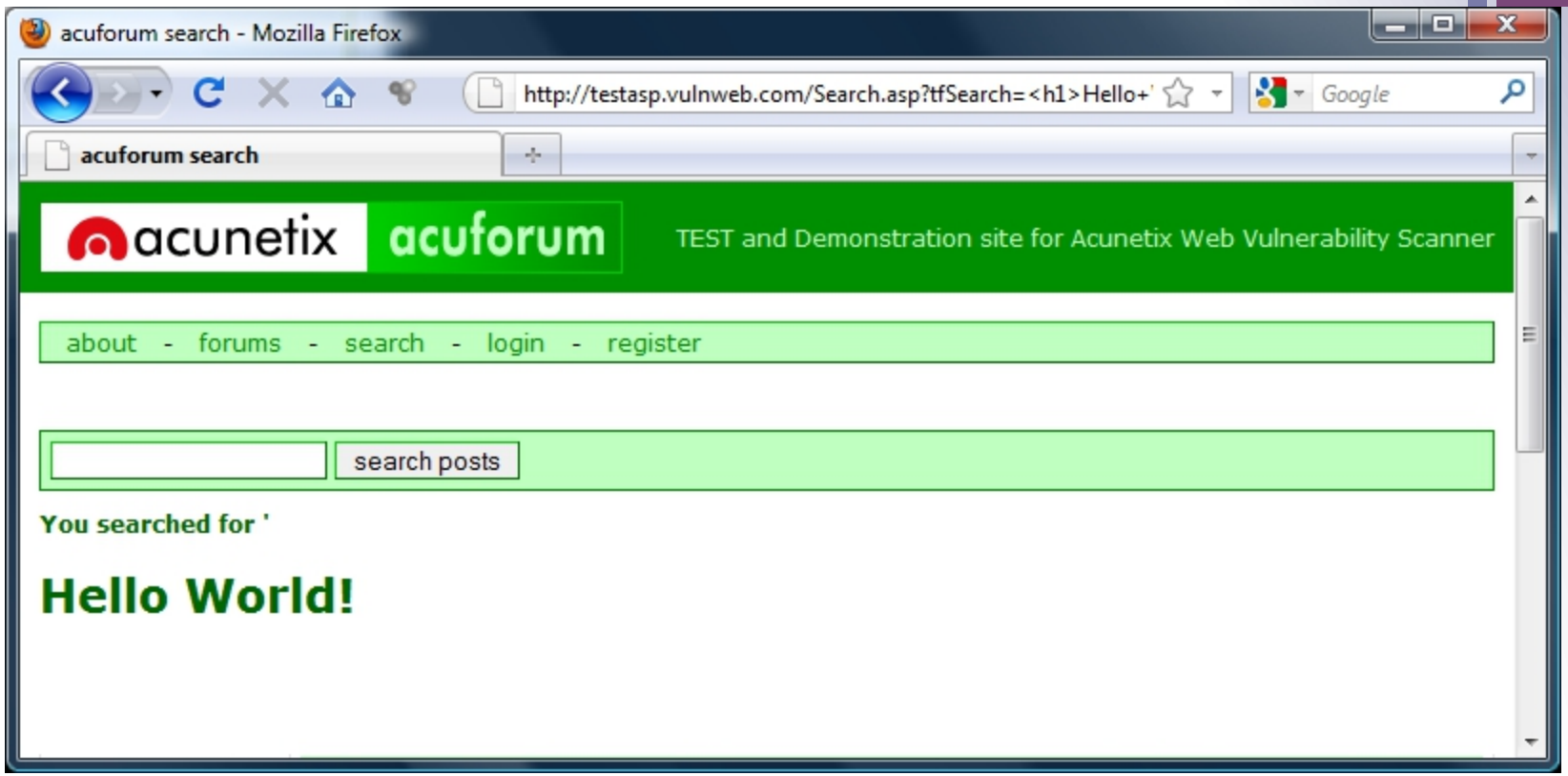
Abusing Web Applications: Example



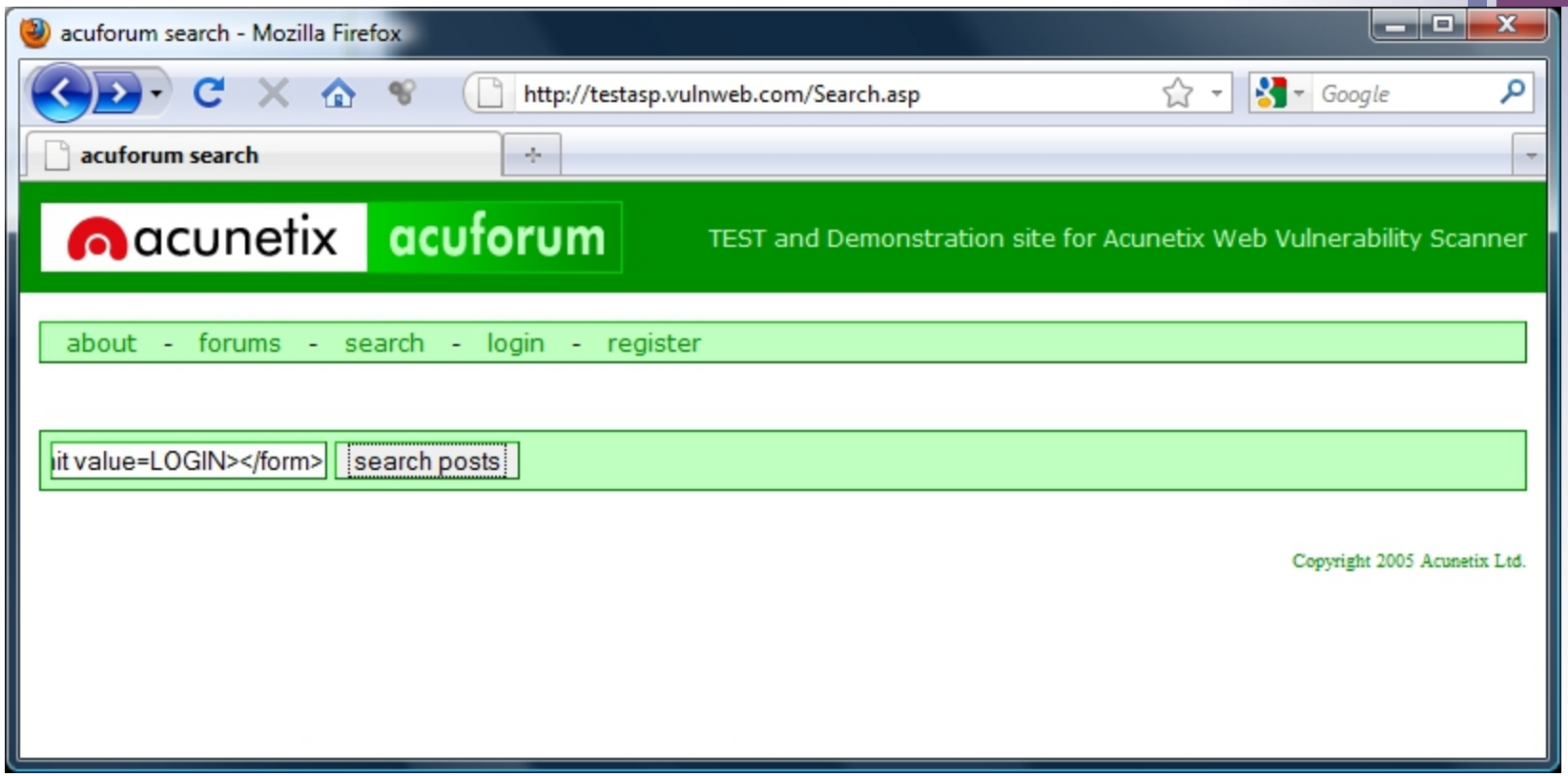
Abusing Web Applications: Example



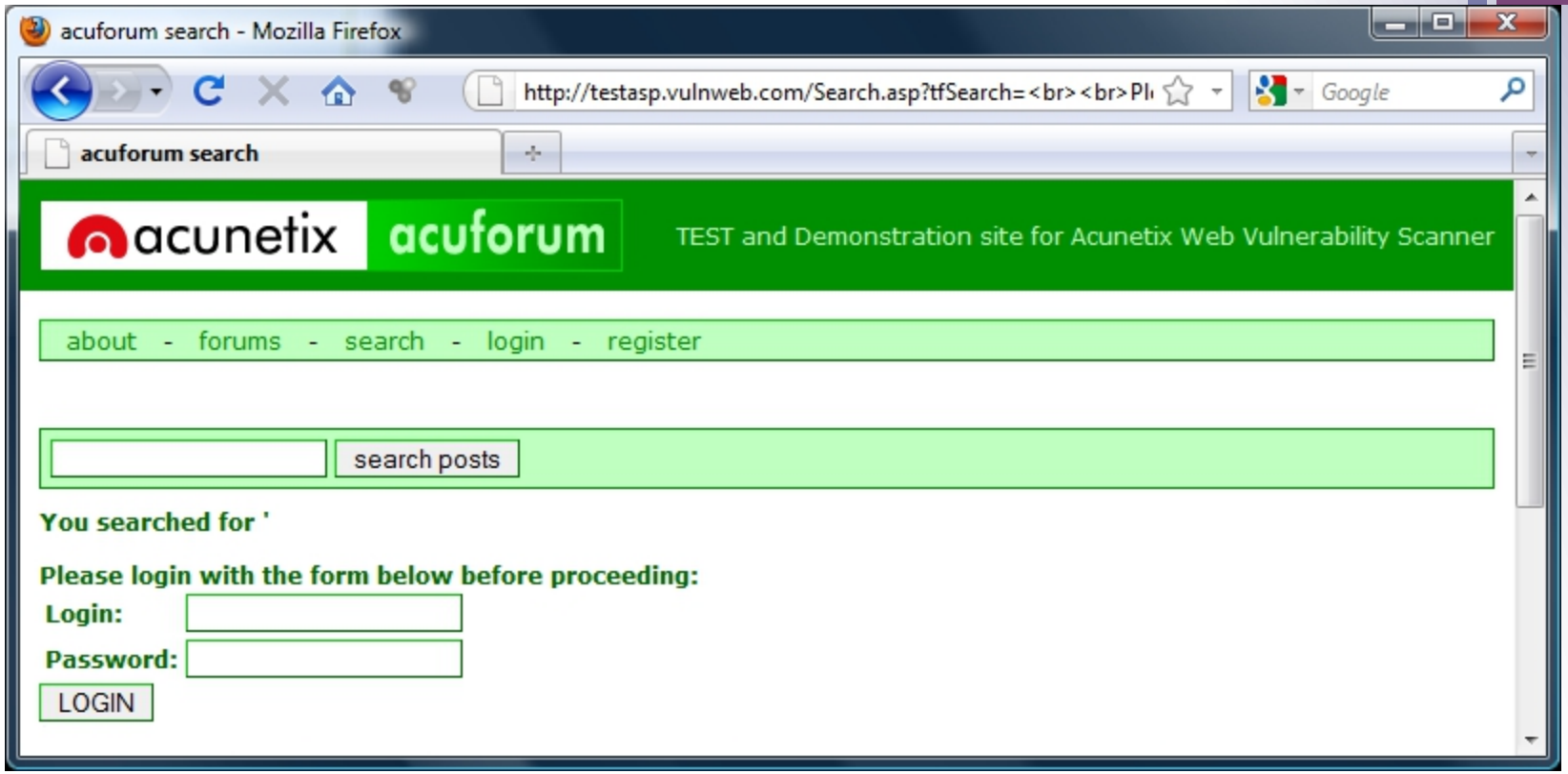
Abusing Web Applications: Example



Abusing Web Applications: Example



Abusing Web Applications: Example

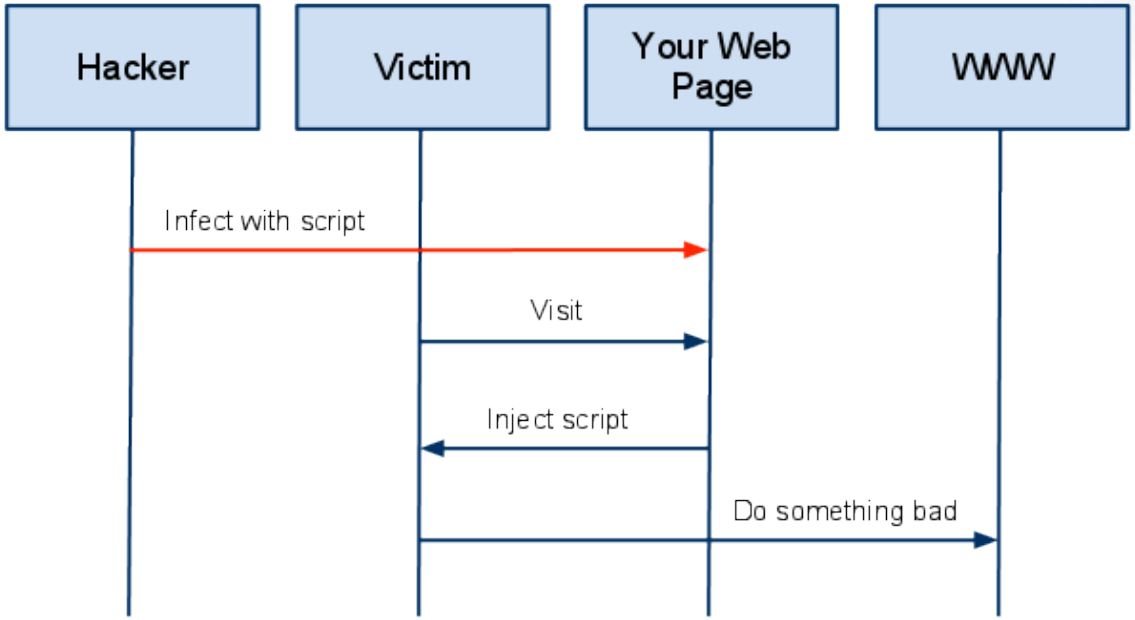



```
<br><br>Please login with the form below before proceeding:<form
action="destination.asp"><table><tr><td>Login:</td><td><input type=text length=20
name=login></td></tr><tr><td>Password:</td><td><input type=text length=20
name=password></td></tr></table><input type=submit value=LOGIN></form>
```

Cross-Site Scripting (XSS)

- Cross-site consists in inserting a script into a web page
- Often, the script itself is located on an other server
  - Cross-site scripting
  - Example <script src="http://www.evilsite.com/hack.js">
- Dangers
  - Session redirecting (e.g. on a copy of the original website)
  - Display fake information or forms to collect data (phishing)
  - Steal cookies
  - Corrupt data

Cross-Site Scripting: General Picture



A High Level View of a typical XSS Attack

Source: http://www.acunetix.com/websitesecurity/xss.htm

Phishing

- Goal is to obtain information and credential by masquerading as a trustworthy entity
- Of the top 20 companies targeted by phishing in 2007, 19 are in the banking industry [IBM]
- Mostly by email
  - Address looks like valid eg www.mybanck.com or http://www.mybank.com.example.com
  - http://www.mybank.com@fakesite.com
  - Hyperlinked Picture
- http://www.antiphishing.org/

SQL Injection

- A web site asks for a username & password
- To authenticate the user from the database, the server uses the input data to construct a SQL query

$query = 'SELECT user, pw FROM users WHERE user = '+ $username+ ' AND pw = '+$password+';"

- The query is executed, and if the result is non-null, the user is authenticated
  - result = run_query($query)
  - if (result != 0) then ok …

SQL Injection

Normal user

- For user = “john” and pw = “1234”, $query is
  - **'SELECT user, pw FROM database WHERE user =**

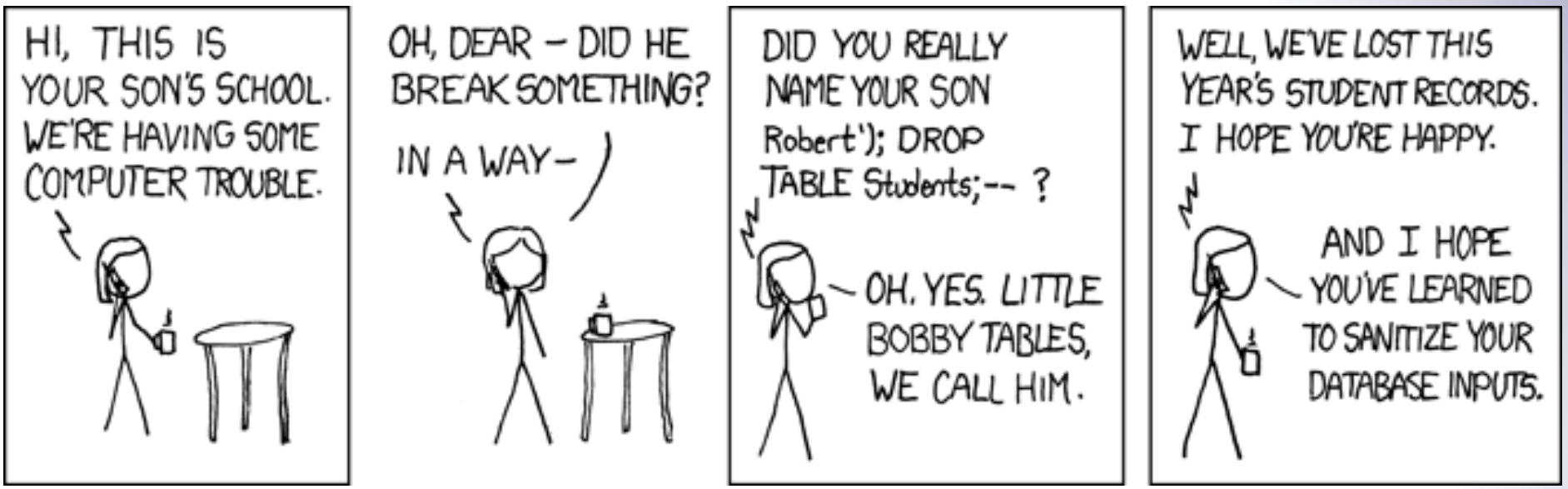
    “john” AND pw = “1234”'

Malicious user

- For user = “admin" /*” and pw = “whatever”, $query is
  - **'SELECT user, pw FROM database WHERE user =**

    “admin" /*” AND pw = “whatever”'
- If admin exists, you can login without password!

Sanitize your database inputs!



xkcd

Buffer Overflow

Buffer Overflow

- If a program doesn't verify the amount of data it receives, it runs the risk of over-writing the memory zone containing variables, code or jump addresses
- Knowing well the machine's architecture, the an attacker can inject machine code that will execute
- >50% of security incidents reported at CERT are related to buffer overflow attacks

Reminder: The Stack

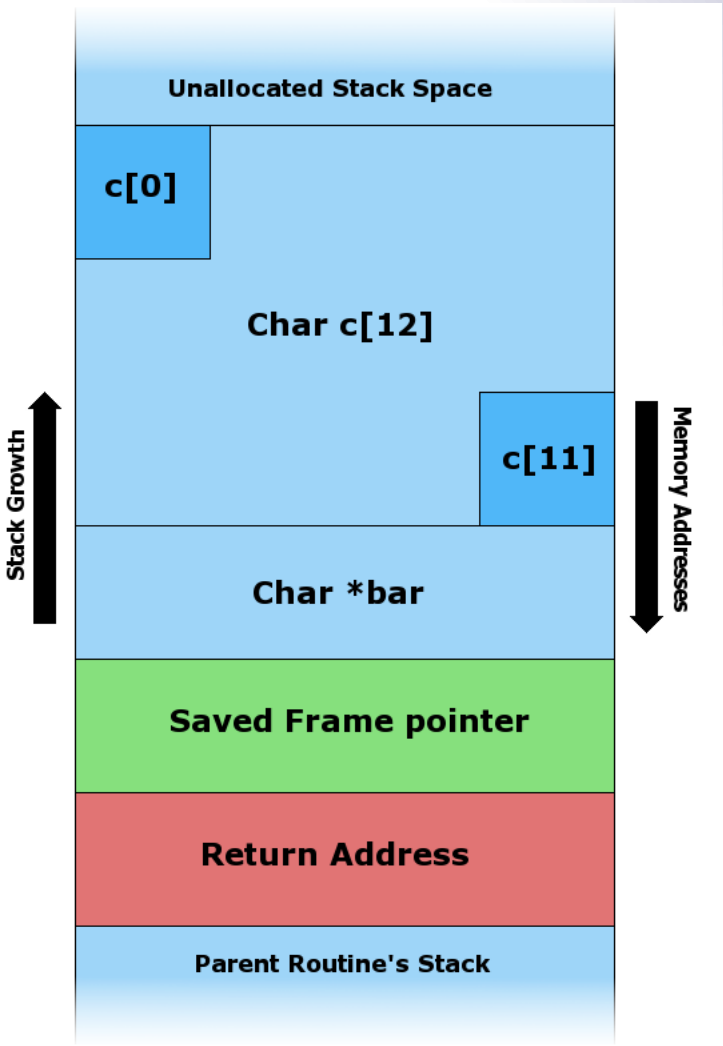
- The stack allows temporary storage of data
- We pop data in the reverse order than when we pushed them
- During a function call, the return address is pushed onto the stack
- We also push the arguments to the function

Reminder: The Stack

- The function's local variables are also pushed onto the stack
- A corresponding zone (the frame) is allocated on the stack
- A frame pointer indicates where the current frame starts on the stack
- During a function call, the previous value of the frame pointer is pushed onto the stack before being replaced by its new value

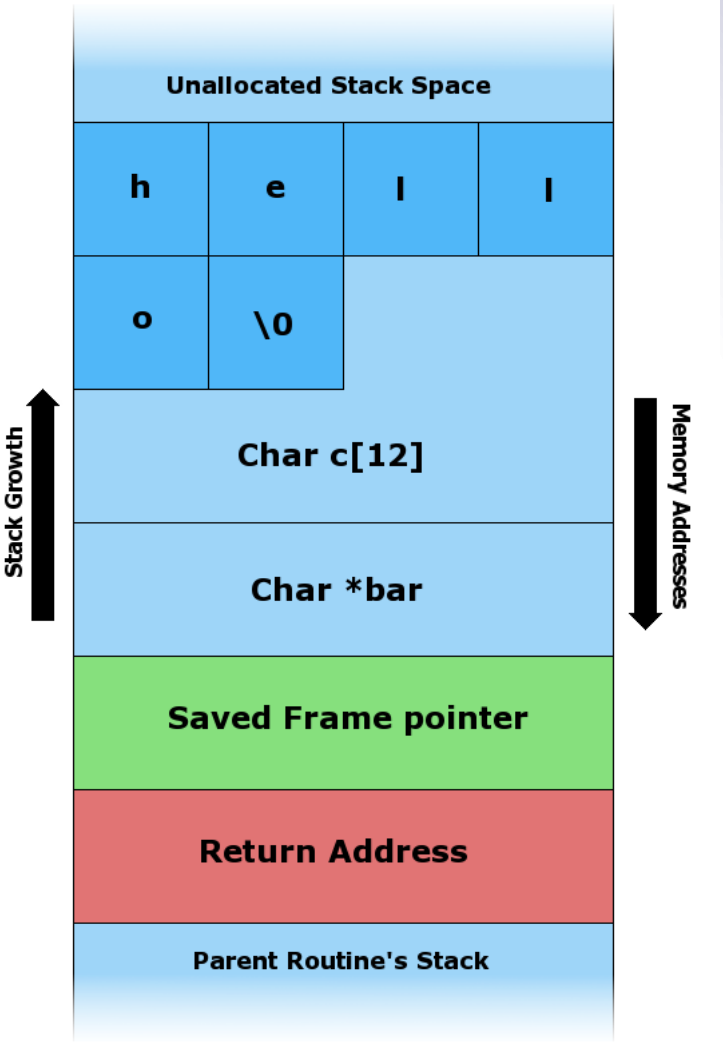
Example [Wikipedia]

```
#include <string.h>
void foo (char *bar)
{
    char c[12];
    memcpy(c, bar, strlen(bar));
    // no bounds checking...
}

int main (int argc, char **argv)
{
    foo(argv[1]);
}
```



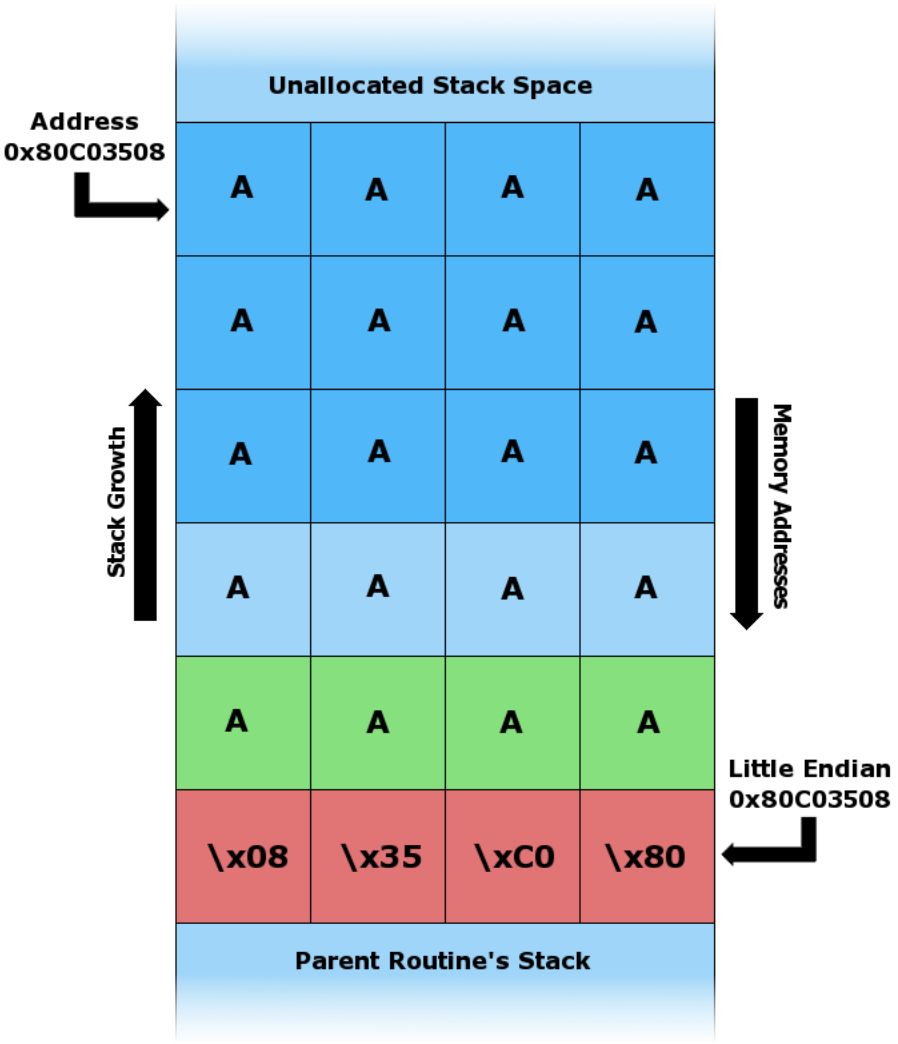
Example [Wikipedia]

```
#include <string.h>
void foo (char *bar)
{
    char c[12];
    memcpy(c, bar, strlen(bar));
    // no bounds checking...
}

int main (int argc, char **argv)
{
    foo(argv[1]);
}
```



Example [Wikipedia]

```
#include <string.h>
void foo (char *bar)
{
    char c[12];
    memcpy(c, bar, strlen(bar));
    // no bounds checking...
}

int main (int argc, char **argv)
{
    foo(argv[1]);
}
```



Difficulties

- It is hard to guess the growth of the stack and choose the address
- The injected machine code may not have a \0 byte, because this signals the end of a character string and prevents copying the remaining bytes

Defeating Buffer Overflows

- Java/C# are not vulnerable to these attacks and memory is garbage collected
- C and C++ programming languages don't do array bounds checks
- If you must use C/C++
  - Avoid broken library routines (e.g., strncpy instead of strcpy)
  - Always do bound checks
  - Manage memory properly
    - Learn modern C++11 features, e.g. shared_ptr, unique_ptr

Code Red Worm, July 2001

- Exploited buffer overflow vulnerability in MS-IIS web server
- Attacker host scans for TCP port 80 and sends exploit string to the victim host
- The worm checks if the victim host was already compromised
- If yes, it stops
- If not, it begins to scan for random IP addresses to infect more serves
- In less than 14 hours, 359,104 hosts were compromised
- More: http://www.caida.org/analysis/security/code-red/

Code Red's exploit

```
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u78
01%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%
u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u00
78%u0000%u00=a
```

Additionally, web pages on victim machines may be defaced with the following message:

HELLO! Welcome to http://www.worm.com!
Hacked By Chinese!

Any questions?

Stay tuned

Next time you will learn about

Network vulnerabilities