Compromised Website Analysis Report

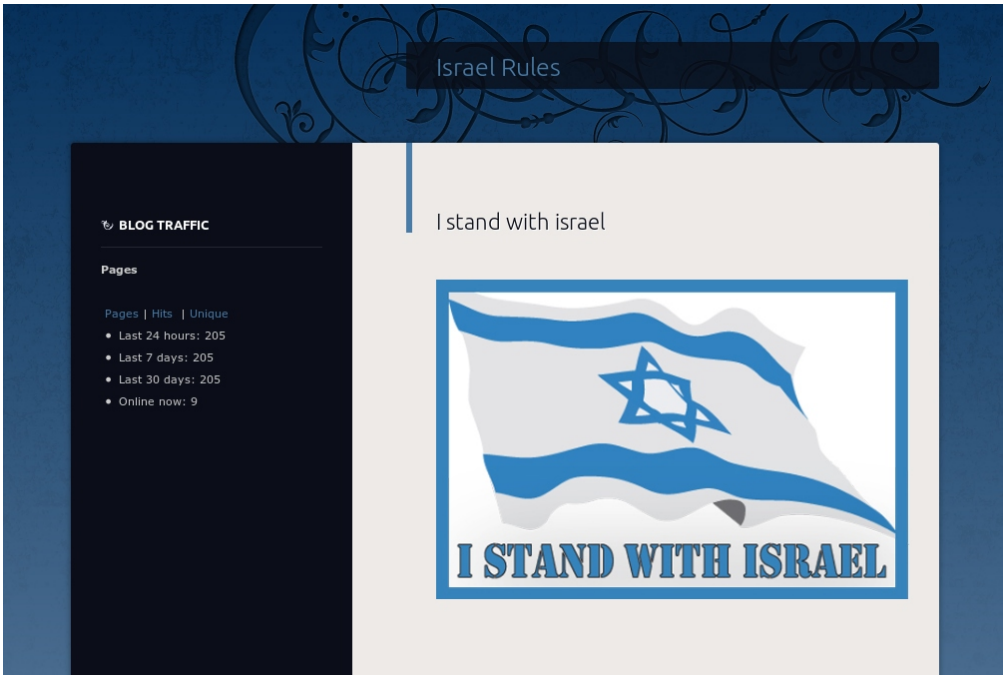
Version: 1.0

Table of Contents

Source Data

Resource: http://www.richardsilverstein.com

It was reported that http://www.richardsilverstein.com was compromised and defaced. On 7 September 2012, around 10:00 AM (UTC) the main webpage was confirmed to be defaced:



The owner of the website has provided full access to the server. Full copy of the website contents including access log files and mysql database dump was obtained for analysis.

Common Facts

The website is running a Wordpress blog engine version 3.4.2, which was the latest available version at the time of analysis.

At the time of analysis the domain www.richardsilverstein.com was resolving to 67.205.15.213.
According to public WHOIS database, the domain information was updated on 06 September 2012.

```
Domain Name: RICHARDSILVERSTEIN.COM
Registrar: ENOM, INC.
Whois Server: whois.enom.com
Referral URL: http://www.enom.com
Name Server: NS1.DREAMHOST.COM
Name Server: NS2.DREAMHOST.COM
Name Server: NS3.DREAMHOST.COM
Status: clientTransferProhibited
Updated Date: 06-sep-2012
```

According to the information on the server filesystem the website was created on 06 September 2012. This is when the webserver log directory was created:

```
  File: `logs'
  Size: 43        Blocks: 0          IO Block: 4096   directory
Device: 811h/2065d   Inode: 12886338779  Links: 3
Access: (0550/dr-xr-x---)  Uid: (13224816/richards1052)   Gid: (  150/dhapache)
Access: 2012-09-06 06:32:04.684628783 -0700
Modify: 2012-09-06 19:00:34.179476532 -0700
Change: 2012-09-07 03:44:01.639843381 -0700
```

According to the first entries in the http access log, the website went online around 06/Sep/2012:21:45:57 -0700.

Website location on the server (webserver root):
/home/richards1052/richardsilverstein.com/tikun_olam

Incident Analysis

The state of the main page of the website indicates that the blog has an entry created by the attacker, which means that the attacker most likely created it using regular methods of adding new blog entry. This proposes an analysis of the database contents and changes as well as access log entries that were added at approximately the same time.

During the analysis, the access credentials to connect and work with the database were picked up from the configuration file of the wordpress: wp-config.php.

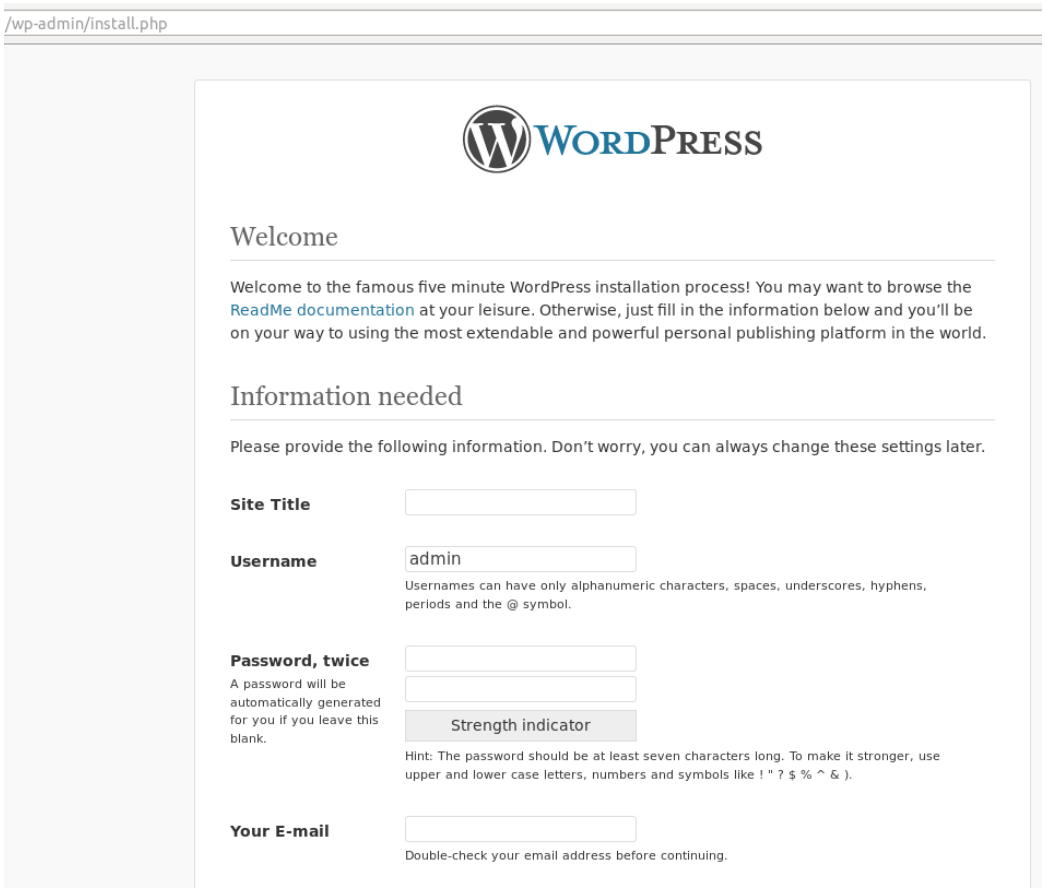
Here is the contents of the posts table (wp_v4qiny_posts):

ID	post_parent	post_author	post_date	post_date_gmt	post_type
1	0	1	2012-09-07 05:49:53	2012-09-07 05:49:53	post
2	0	1	2012-09-07 05:49:53	2012-09-07 05:49:53	page
3	0	1	2012-09-07 05:50:09	0000-00-00 00:00:00	post
4	0	1	2012-09-07 05:50:26	0000-00-00 00:00:00	post
5	2	1	2012-09-07 05:52:38	2012-09-07 05:52:38	revision
6	2	1	2012-09-07 05:49:53	2012-09-07 05:49:53	revision
7	2	1	2012-09-07 05:53:59	2012-09-07 05:53:59	revision
8	1	1	2012-09-07 05:49:53	2012-09-07 05:49:53	revision

The attacker logged in and modified post with ID 2 which produced revision records with ID 5 and 7 and inserted the following content:

The first entry, which was added to the table 3 minutes before the attacker placed his own content and it indicates when the blog engine was initialized. This should correlate with http access log.

Since 06/Sep/2012:21:48:58 -0700 some of the website visitors were redirected to www.richardsilverstein.com/wp-admin/install.php which displayed an installation web page for the visitor:



This webpage is normally displayed to the owner of the blog after passing the first stage of Wordpress installation which requires entering the database login and password. If the Wordpress doesn't find its config file (wp-config.php) it will redirect the visitor to /wp-admin/setup-config.php. However, according to the access logs /wp-admin/setup-config.php has never been accessed, which means that the Wordpress config was created by something else. If the Wordpress was installed via some website control panel (or any site management interface) then the scripts of the control panel are responsible for creating Wordpress config and setting the database credentials in the config. This opens a security breach, because after the owner of the website installs Wordpress and before he accesses /wp-admin/install.php to complete Wordpress setup, the attacker can get there and enter his own credentials for website admin and get full control for the blog (including ability to post anything).

wp-config.php file was discovered in the webserver root directory and had the following attributes:

```
  File: `wp-config.php'
  Size: 3593            Blocks: 8          IO Block: 4096   regular file
Device: 811h/2065d   Inode: 8593611962  Links: 1
Access: (0640/-rw-r-----)  Uid: (13224816/richards1052)   Gid: (1054392/pg5455029)
Access: 2012-09-06 19:03:03.000000000 -0700
Modify: 2012-09-06 19:03:03.000000000 -0700
Change: 2012-09-06 19:03:20.238447628 -0700
```

This reveals that the Wordpress was partly installed by the website owner around 2012-09-06 19:03:03 UTC-7, and remained in incomplete installation state until discovered by the attacker at 06/Sep/2012:22:49:52 UTC-7.

The following record from access log confirms this:

109.64.243.116 - - [06/Sep/2012:22:49:52 -0700] "**POST /wp-admin/install.php?step=2** HTTP/1.1" 200 1034 "http://www.richardsilverstein.com/wp-admin/install.php" "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.4 (KHTML, like Gecko) Chrome/22.0.1229.26 Safari/537.4"

The attacker completed Wordpress installation and got a full control over the blog. The IP address of the attacker according to the access logs is 109.64.243.116.

After completing the installation, the attacker logs in to the Wordpress interface, creates and modifies blog entries:

109.64.243.116 - - [06/Sep/2012:22:50:06 -0700] "**POST /wp-login.php** HTTP/1.1" 302 1107 "http://www.richardsilverstein.com/wp-login.php" "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.4 (KHTML, like Gecko) Chrome/22.0.1229.26 Safari/537.4"

109.64.243.116 - - [06/Sep/2012:22:50:26 -0700] "**GET /wp-admin/post-new.php** HTTP/1.1" 200 14742 "http://www.richardsilverstein.com/wp-admin/edit.php?orderby=title&order=asc" "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.4 (KHTML, like Gecko) Chrome/22.0.1229.26 Safari/537.4"

109.64.243.116 - - [06/Sep/2012:22:53:59 -0700] "**GET /wp-admin/post.php?post=2&action=edit&message=1** HTTP/1.1" 200 13544 "http://www.richardsilverstein.com/wp-admin/post.php?post=2&action=edit" "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.4 (KHTML, like Gecko) Chrome/22.0.1229.26 Safari/537.4"

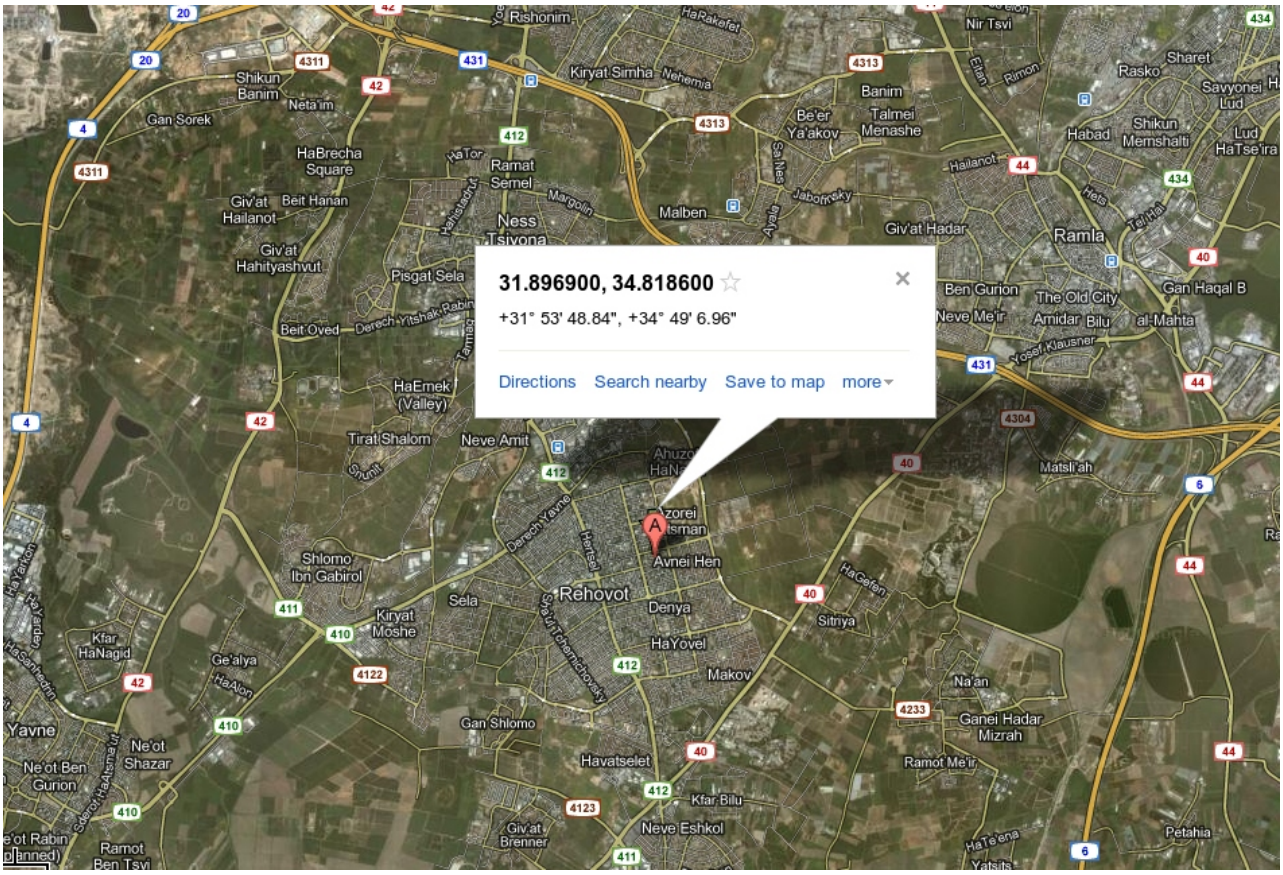
The time of last edit matches the time saved in the mysql database, table posts (note the different timezone):
2012-09-06 22:53:59 **UTC-7** == 2012-09-07 05:53:59 **UTC**

Finally the attacker visits the main webpage several times. The last visit log entry:
109.64.243.116 - - [06/Sep/2012:23:13:23 -0700] "**GET /** HTTP/1.1" 200 4280 "http://webcache.googleusercontent.com/search?q=cache:9EFnhC0Rx_gJ:www.richardsilverstein.com/+&cd=1&hl=ru&ct=clnk&gl=il" "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.4 (KHTML, like Gecko) Chrome/22.0.1229.26 Safari/537.4"

The Attacker Info

Logged attacker IP: 109.64.243.116
Last timestamp when IP was used: 06/Sep/2012 23:13:25 -0700

GeoIP information (https://www.maxmind.com/app/locate_demo_ip?ips=109.64.243.116):



Please mind tha thet real GeoIP location of the attacker can be different due to various factors.

IP: **109.64.243.116**
Country: **Israel**
Region: **HaMerkaz**
City: **Rehovot**
Latitude: **31.8969**
Longitude: **34.8186**
ISP: **Bezeq International**
Organization: **Bezeq International**

WHOIS information:
inetnum: 109.64.0.0 - 109.64.255.255
netname: BEZEQINT-BROADBAND

descr: *SE1-PTK*
country: IL
admin-c: BNT1-RIPE
tech-c: BHT2-RIPE
status: ASSIGNED PA
remarks: We are more than NO. 1
remarks: please send ABUSE complains to abuse@bezeqint.net
mnt-by: AS8551-MNT
mnt-lower: AS8551-MNT
source: RIPE # Filtered

role: BEZEQINT HOSTMASTERS TEAM
address: Bezeq International
address: 40 hashacham st.
address: Petach Tikva 49170 Israel
phone: +972 1 800014014
fax-no: +972 3 9257674
admin-c: MR916-RIPE
tech-c: LBHM-RIPE
tech-c: HMSB-RIPE
nic-hdl: BHT2-RIPE
remarks: Please Send Spam and Abuse ONLY to abuse@bezeqint.net
mnt-by: AS8551-MNT
source: RIPE # Filtered

role: BEZEQINT NETWORKING TEAM
address: Bezeq International
address: 40 hashacham st.
address: Petach Tikva 49170 Israel
phone: +972 1 800014014
fax-no: +972 3 9257674
admin-c: MR916-RIPE
tech-c: MR916-RIPE
tech-c: RD1278-RIPE
nic-hdl: BNT1-RIPE
remarks: Please Send Spam and Abuse ONLY to abuse@bezeqint.net
mnt-by: AS8551-MNT
source: RIPE # Filtered

Additionally Wordpress requires inputting a valid email address for the admin. It is not later verified, however the address should comply with the standards. If the attacker wasn't familiar with Wordpress, he could enter his real email, in case the Wordpress verifies it later to let the attacker log in as admin.

This could explain what was discovered in the table of blog users:

```
+------------+---------------------+-------------------+
| user_login | user_registered     | user_email        |
+------------+---------------------+-------------------+
| admin      | 2012-09-07 05:49:53 | semkras@gmail.com |
+------------+---------------------+-------------------+
```

The e-mail address of the potential attacker or a person associated with him: **semkras@gmail.com**

Some webpages containing a reference to semkras@gmail.com.

http://lazareus.wikidot.com/work

The attacker most likely speaks Russian:
http://rabota-il.livejournal.com/4972662.html?nojs=1

Probably has a kid:
http://mnews.co.il/forum/forum_posts.asp?TID=147&PN=20

In 2009 claimed to live in Modi'in:
http://orbita-sat.com/forum/showthread.php?t=678&page=3&langid=1

Youtube channel:
https://www.youtube.com/user/semkras

The Youtube channel reveals a name of person associated with the potential attacker: Аркадий Красильщиков (Arkadiy Krasilschikov), Russian-speaking jewish born in St.Petersburg.

Twitter account:
https://twitter.com/semkras

Further Steps

It is highly recommended to completely remove all current files from the webserver and clean the mysql database.

The installation of Wordpress using current webhosting site management system should be done with proper IP filtering applied, so that no one can access the webserver until the Wordpress installation is complete and the webserver is fully configured.

Additionally, it is recommended (if allowed by the hosting company) to disable or apply IP filtering for the network services that are running on the same host, which should leave only those services that are used by the resource (i.e. webserver, port 80).

Nmap scan report for richardsilverstein.com (67.205.15.213)

```
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
587/tcp  open  submission
5222/tcp open  unknown
5269/tcp open  unknown
```

It is critical to use passwords that are complex and hard to bruteforce/guess, different for accessing various resources.