

The return of SIMBAR

Cyber-terrorism methodology

by Kfir Damari and Andre Oboler
kfird@beyondsecurity.com, oboler@ZionismOnTheWeb.org



Overview

In early July 2006 we [wrote an analysis](#) of a defacement against a web server, during the Team Evil attack spree against pro-Israeli servers in the cyber terrorism aftermath of Israeli operations in the Gaza strip.

Shortly after we released the report we received an email requesting assistance with an ongoing attack.

This case study is based on an attack on a shared hosting server, and specifically www.zionismontheweb.org.

This article was co-written with Andre Oboler, administrator of "Zionism On The Web" and a PhD Candidate in the Computing at Lancaster University, UK.

Scope and purpose of this document

This text will compare latest defacement incidents with the incident we responded to in July, and will describe Team Evil's Hacking methodology. This analysis aims to provide with an insight to the modus operandi of youth Cyber



beSIRT

terrorism groups.

The information presented in this text was gathered from various sources, and particularly log analysis.

As a secondary goal, in this text we will also demonstrate how such incidents can be investigated and provide with educational comments on how the data analyzed can be approached.

Team Evil - Background

“Team Evil” is a cyber-terrorism group that claims to be based in Marroco. The group does not focus on specific targets, and most of the time simply attacks targets of opportunity. Some high profile [hacks](#) include government sites in Israel, Jordan, Saudi Arabia, Bahrain, France, Paraguay, Costa Rica, the Ivory Coast, Argentina, Colombia and others.

In a recent [interview with Ynet News](#) a spokesperson for the group said they were all "Moroccan youths, under the age of 20", he also claimed that hacking was not illegal.

Attack Details

“Team Evil” hacked and defaced the site's main page, as well as its forum, blogs and photo gallery. Finally they corrupted the database and folders on the server.

After the initial attack, security measures were employed by the site's administrator. Team Evil apparently became agitated, and retaliated with destructive measures. Eventually they deleted files essential to the site's operation, renamed folders to obscene names, etc. (See Illustration 3). As only the administrator of the site would see the renamed folders, it is possible that the attack became personal for Team Evil.

Over the period of a month, the site was constantly under attack. Every time administrators restored the site (and closed security holes), Team-Evil attacks escalated.

For a complete attack description, see Appendix A.

Screen captures of attack results

Illustration 1: Results of second attack on zionizmontheweb.org



*Illustration 2: Defaced front page.
Note the Allah Akbar in the title bar.*





beSIRT

Attack Analysis

Team-Evil used web-based vulnerabilities to install backdoor tools on the server. As the site was part of a shared hosting server, tools installed were used to attack other sites on the same server.

The Vulnerabilities Exploited

- Software: PhPBB Forum Software
Vulnerability: Remote code execution. Used Inadequate UTF-8 character escaping to execute a shell script hosted in another server.
- Software: B2Evolution Blogs Software
Vulnerability: Insecure installation. Team-Evil had direct access to configuration scripts in default directories.
- Software: Coppermine Photo Gallery
Vulnerability: Remote file inclusion. Uploaded file was a JPG with embedded PHP inside.
- It seems Team-Evil also hacked other sites hosted on the same server. Full logs were not available, so the exact exploits used are unknown.
- Non of the vulnerabilities were 0day, and a patch existed for all of them.

The attackers use multiple tools during this attack. You can find more information about them in Appendix B.

The Analysis Process: Log Analysis

The site administrator provided with suspicious IP addresses accessing the site. It seems the majority of the attacks came from a university in Saudi Arabia, specifically from: 212.138.47.* , 212.138.64.* and 212.138.113.*

Another clue was "SIMBAR". In our previous [case study](#), the intruder's computer was infected with a spyware which adds "SIMBAR" to the user agent of Internet Explorer. The logs for this attack showed the same, indicating that the same computer may have been used in both attacks.



Sample 1: Logs showing attacker had SIMBAR added to the user agent

```
361279 212.138.113.25 - - [08/Aug/2006:00:45:14 +0100]
```

```
"GET / HTTP/1.0" 200 48429
```

```
"http://giyus.org/?bn=bn_solid_tiny" "Mozilla/4.0 (compatible;  
MSIE 6.0; Windows NT 5.1; SV1; SIMBAR Enabled; .NET CLR  
1.1.4322)"
```

As mentioned, Team Evil's arsenal is built mainly of web attack tools. This makes things simpler as the exploit will probably be saved in the web server log.

Searching the log files for "SIMBAR" resulted with interesting URLs:

- GET /blogs/config.php HTTP/1.0
- GET /blogs/b2evocore/_main.php HTTP/1.0
- GET //blogs/.help.php?act=ls&d=%2Fhome%2Fvsvkdg%2Fpublic_html%2F&sort=0a HTTP/1.0

The first two lines indicate the attacker (named from here on *SIMBAR*), tried to access the blogs configuration scripts.

The last GET request executes a directory listing for:

/home/vsvkdg/public_html/, using a tool the hacker uploaded.

In the logs there were entries to multiple unknown files, which were uploaded by the attackers. Two examples are:

- /blogs/.help.php
- /boards/images/smiles/smlis.gif

Some of these files were plain PHP scripts while some were pictures embedded with PHP code ([concatenated to the end of the picture](#)). For more information see Appendix B. While these files were deleted, the logs were searched for the first occurrence to find how these files were uploaded.



The Analysis Process: Analysis Conclusions

It seems that one of the attackers, *SIMBAR* was the first to enter the site. The referrer column in the logs shows: `http://giyus.org/?bn=bn_solid_tiny`

We found four other Agent Id's involved in the defacement, suggesting multiple attack sources. *SIMBAR* installed most of the exploit tools, while another attacker ran the SQL commands on the database.

The intruders installed scripts on other sites hosted on the server as shown below

Sample 2: Logs showing attacker using the exploit on another site on the same shared hosting server

```
83.101.150.116 - - [11/Sep/2006:21:35:52 +0100] "GET
/hackers/images/ZOTW_hack2.png HTTP/1.1" 403 -
"http://www.example.com/.help.php?act=f&f=christians.html
&d=%2Fhome%2Fvsvkdg%2Fpublic_html%2Fblogs&" "Mozilla/4.0
(compatible; MSIE 6.0;
```

We found different SQL statements that were executed. Here is an example:

Sample 3: Logs showing SQL commands used by the backdoor tool

```
"http://www.zionisontheweb.org/gallery/include/Titan.php
?act=sql&sql_login=user&sql_passwd=pass&sql_server=localh
ost&sql_port=3306&sql_db=db_name&sql_tbl_act=insert
&sql_tbl=cpg_users&sql_tbl_ls=0&sql_tbl_le=30
&sql_tbl_insert_q=+'user_id`+=+'1'+AND+'user_group`+=+'1'
+AND+'user_active`+=+'YES'+AND+'user_name`+=+'spooft'+AND+
'user_password`+=+'some_hash'+AND+'user_lastvisit`+=+'200
6-05-11+20:16:44'+AND+'user_regdate`+=+'2006-05-
11+20:16:21'+AND+'user_group_list`+=+''+AND+'user_email`+
+=+'spooft@zionisontheweb.org'+AND+'user_profile1`+=+''+AN
D+'user_profile2`+=+''+AND+'user_profile3`+=+''+AND+'user
_profile4`+=+''+AND+'user_profile5`+=+''+AND+'user_profil
e6`+=+''+AND+'user_actkey`+=+''+"
```

This SQL statement in the sample above, updates a user account in the



beSIRT

database, in this case it looks like the purpose was to replace the users' password hash.

From referrers in the log we learned the attackers spoke of the attack publicly:

- <http://www.moqawmh.com/vb/showthread.php?p=41320#post41320>
- <http://www.tryag.com/vb/showthread.php?t=7468>
- <http://www.tryag.com/vb/showthread.php?p=83949#post8394>



Conclusions and methodology

Using the information gathered we can try to characterize the way “Team Evil” operates:

1. Use known web vulnerabilities to install web based backdoor tools.
2. Find & gain all administrator passwords (Site, Database, management panel, etc.)
3. Install backdoor tools on all other sites on the shared hosting server.
4. Defacement (often by redirecting to an old one at Zone-H).

Looking at “Team Evil”, they seem more like script kiddies then hardcore hackers. Never the less, they are rated 47 in [zone-h Attackers Top List](#), with 8084 known defacements. Meaning their methodology might not be sophisticated, but it serves their goal and they’ve mastered the tools and exploits they choose to use.

With a few simple actions one can probably prevent most of the attacks:

- Stay updated, most of the known vulnerabilities are patched quickly. If the software vendor you use doesn't fix the problems, see if you can change a vendor.
- Make sure you change all your passwords frequently.
- When installing web based applications such as forums, it is better not to use the default installation directories and file names.
- Don't run your web daemon with root permissions.
- Delete all files you don't use.
- Avoid shared hosting if at all possible.

In conclusion, Team Evil are very successful at defacing sites. Their tools and techniques are not very advanced, but they work.

They do not seem to have advanced much since our last case study, they use a new tool but their methodology remains the same, and the tool is not one they built on their own.

"Perfection is achieved, not when there is nothing more to add, but when there is nothing left to take away." (- Antoine de Saint Exupery)



beSIRT

Appendix A – Attack Description Chronologically

First Attack Wave

Forum and front page defacement (See Illustration 2).

Second Attack

Forum and front page defacement. Site's configuration was manipulated so anti Israeli messages are displayed (See Illustration 4).

Third, Fourth and Fifth Attacks

Users' database was defaced and later emptied. As a final blow database was dropped entirely.

Sixth Attack

Admin account was taken over. All user names on the forum were changed to "Team Evil". As before, insulting messages were added and pages were defaced.

Seventh Attack

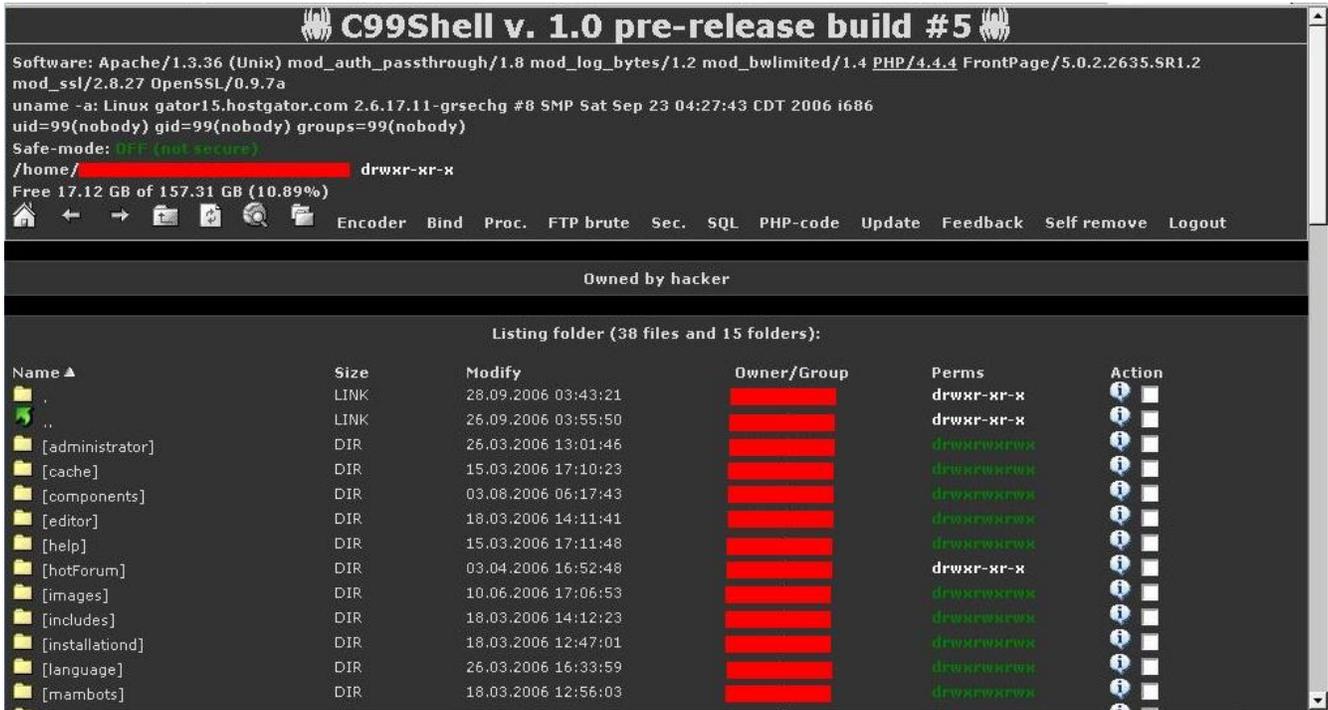
Forum and front page defacement. Database was trashed for both the blogs and forum systems.
This time Team-Evil managed to change the forum name without using the admin panel (which was removed after previous attacks).

Eighth Attack

A week after previous attacks, exploited vulnerabilities were sealed and planted tools have been completely removed.
Team-Evil attacked again. This time renamed folders, wiped one databases almost completely, and opted not just to deface the system but to destroy as much of it as they could (See Illustration 3).



Appendix B – The tools used



- C99Shell–
 - ① Coded by: tristram [CCTeam - Captain Crunch Security Team].
 - ① Version Used: 1.0 pre-release build #5
 - ① Type: Graphic Remote Shell (Hacking remote console)
 - ① Feathers:
 - Host Information
 - Directory listing
 - Execute shell command:
 - find all suid files - "find / -type f -perm -04000 -ls"
 - find suid files in current dir - "find . -type f -perm -04000 -ls"
 - find all sgid files - "find / -type f -perm -02000 -ls"
 - find sgid files in current dir - "find . -type f -perm -02000 -ls"
 - find config.inc.php files - "find / -type f -name config.inc.php"
 - find config* files - "find / -type f -name \"config*\""
 - find config* files in current dir - "find . -type f -name \"config*\""
 - find all writable folders and files - "find / -perm -2 -ls"
 - find all writable folders and files in current dir - "find . -perm -2"



beSIRT

- ls"
- find all service.pwd files - "find / -type f -name service.pwd"
- find service.pwd files in current dir - "find . -type f -name service.pwd"
- find all .htpasswd files - "find / -type f -name .htpasswd"
- find .htpasswd files in current dir - "find . -type f -name .htpasswd"
- find all .bash_history files - "find / -type f -name .bash_history"
- find .bash_history files in current dir - "find . -type f -name .bash_history"
- find all .fetchmailrc files - "find / -type f -name .fetchmailrc"
- find .fetchmailrc files in current dir - "find . -type f -name .fetchmailrc"
- list file attributes on a Linux second extended file system - "lsattr -va"
- show opened ports - "netstat -an | grep -i listen"
- Costume Command
 - Search file (using regexp)
 - Upload file
 - Create Directory
 - Download / Open a file
 - Create a text file
- r57shell
 - ① Coded by:
 - ① Version: 1.31 – This is the last version. It was also used in our previous case study.
 - ① Type: Graphic Remote Shell (Hacking remote console)
 - ① Feathers:
 - Host Information
 - Directory listing
 - Execute shell command:
 - All commands C99 Commands.
 - find .mysql_history files in current dir - "find . -type f -name .mysql_history"
 - Search file (using regexp)
 - Upload file to the server from user computer
 - Upload file to the server from a http address
 - Download / Open a file.
 - Create a text file
 - Connect to an ftp and download/ upload files
 - Execute a binary file



beSIRT

- Executing php commands
- Sending an email and attaching a file from the server
- Connect to a MySql server and run sql commands
- Brute force to an ftp server using user names from /etc/passwd
- Remote shell and Connect-Back shell
- Create a proxy server
- ① Tool obtained from site: <http://rst.void.ru>

- ZETHA WEB SHELL –
 - ① Coded by: *Loader* and Modify By xMs3D0.
 - ① Also used in our previous case study.
 - ① Type: Graphic Remote Shell (Hacking remote console)
 - ① Feathers:
 - Directory listing
 - Upload file to the server from user computer
 - Upload file to the server from a http address
 - Bind a binary to a specific port
 - Download / Edit a file
 - ① Source and screen shot can be found at the previous case study.

- goo.php
 - ① Coded by: *rgod*
 - ① Version: v.2.1
 - ① Type: Google scanner
 - ① Tool obtained from site: <http://retrogod.altervista.org>

- mwic.php
 - ① Coded By: Seemed to be written by Team Evil.
 - ① Type: Remote php file include.

Drawing 1: mwic.php source code