## 问题描述

当内存马伪造成 `org.apache.catalina` 包名下的类时，会出现异常。

异常堆栈：

```
java.lang.reflect.InvocationTargetException
    at sun.reflect.NativeConstructorAccessorImpl.newInstance0(Native Method)
    at
sun.reflect.NativeConstructorAccessorImpl.newInstance(NativeConstructorAccessorImpl.java
:62)
    at
sun.reflect.DelegatingConstructorAccessorImpl.newInstance(DelegatingConstructorAccessorI
mpl.java:45)
    at java.lang.reflect.Constructor.newInstance(Constructor.java:423)
    at
org.apache.commons.lang.gw.SerializationUtil.addFilter(TomcatFilterInjectorTpl.java:155)
    at org.apache.commons.lang.gw.SerializationUtil.<init>
(TomcatFilterInjectorTpl.java:35)
    at sun.reflect.NativeConstructorAccessorImpl.newInstance0(Native Method)
    at
sun.reflect.NativeConstructorAccessorImpl.newInstance(NativeConstructorAccessorImpl.java
:62)
    at
sun.reflect.DelegatingConstructorAccessorImpl.newInstance(DelegatingConstructorAccessorI
mpl.java:45)
    at java.lang.reflect.Constructor.newInstance(Constructor.java:423)
    at java.lang.Class.newInstance(Class.java:442)
    at org.apache.jsp.defineClass_jsp.defineClazz(defineClass_jsp.java:28)
    at org.apache.jsp.defineClass_jsp._jspService(defineClass_jsp.java:151)
    at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:71)
    at javax.servlet.http.HttpServlet.service(HttpServlet.java:733)
    at org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:477)
    at org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:385)
    at org.apache.jasper.servlet.JspServlet.service(JspServlet.java:329)
    at javax.servlet.http.HttpServlet.service(HttpServlet.java:733)
    at
org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.
java:231)
    at
org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166
)
    at org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:53)
    at
org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.
java:193)
```

```
    at
org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166
)
    at
org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:202)
    at
org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:97)
    at
org.apache.catalina.authenticator.AuthenticatorBase.invoke(AuthenticatorBase.java:542)
    at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:143)
    at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:92)
    at
org.apache.catalina.valves.AbstractAccessLogValve.invoke(AbstractAccessLogValve.java:690
)
    at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:78)
    at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:343)
    at org.apache.coyote.http11.Http11Processor.service(Http11Processor.java:374)
    at org.apache.coyote.AbstractProcessorLight.process(AbstractProcessorLight.java:65)
    at
org.apache.coyote.AbstractProtocol$ConnectionHandler.process(AbstractProtocol.java:888)
    at
org.apache.tomcat.util.net.NioEndpoint$SocketProcessor.doRun(NioEndpoint.java:1597)
    at org.apache.tomcat.util.net.SocketProcessorBase.run(SocketProcessorBase.java:49)
    at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
    at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
    at
org.apache.tomcat.util.threads.TaskThread$WrappingRunnable.run(TaskThread.java:61)
    at java.lang.Thread.run(Thread.java:748)
Caused by: java.lang.ClassNotFoundException: org.apache.catalina.Suo5Filter
    at java.net.URLClassLoader.findClass(URLClassLoader.java:382)
    at java.lang.ClassLoader.loadClass(ClassLoader.java:418)
    at java.lang.ClassLoader.loadClass(ClassLoader.java:351)
    at
org.apache.catalina.core.DefaultInstanceManager.loadClass(DefaultInstanceManager.java:52
9)
    at
org.apache.catalina.core.DefaultInstanceManager.loadClassMaybePrivileged(DefaultInstance
Manager.java:520)
    at
org.apache.catalina.core.DefaultInstanceManager.newInstance(DefaultInstanceManager.java:
150)
    at
org.apache.catalina.core.ApplicationFilterConfig.getFilter(ApplicationFilterConfig.java:
249)
    at org.apache.catalina.core.ApplicationFilterConfig.<init>
(ApplicationFilterConfig.java:102)
    ... 41 more
```

## 异常原因

- org.apache.catalina.core.DefaultInstanceManager#loadClass

```
protected Class<?> loadClass(String className, ClassLoader classLoader) throws
ClassNotFoundException {
  if (className.startsWith("org.apache.catalina")) {
      return this.containerClassLoader.loadClass(className);
  } else {
      try {
          Class<?> clazz = this.containerClassLoader.loadClass(className);
          if (ContainerServlet.class.isAssignableFrom(clazz)) {
              return clazz;
          }
      } catch (Throwable var4) {
          ExceptionUtils.handleThrowable(var4);
      }

      return classLoader.loadClass(className);
  }
}
```

包名为 org.apache.catalina 时用的是加载器 containerClassLoader ，而 defineclass 使用的 当前线程的上下文 classloader，这样会导致 defineclass使用的classloader 和 load suo5filter 的classloader 不是一个，所以会 classnotfound

包名不是 org.apache.catalina 时，也会先走一遍上面的类加载流程，但是不同的在于多了一个 try catch；当 containerClassLoader 加载不到时，会使用 ParallelWebappClassLoader 进行加载，而该 classloader 正好是注入器所用来defineclass 的加载器 Thread.currentThread().getContextClassLoader()，所以正常加载

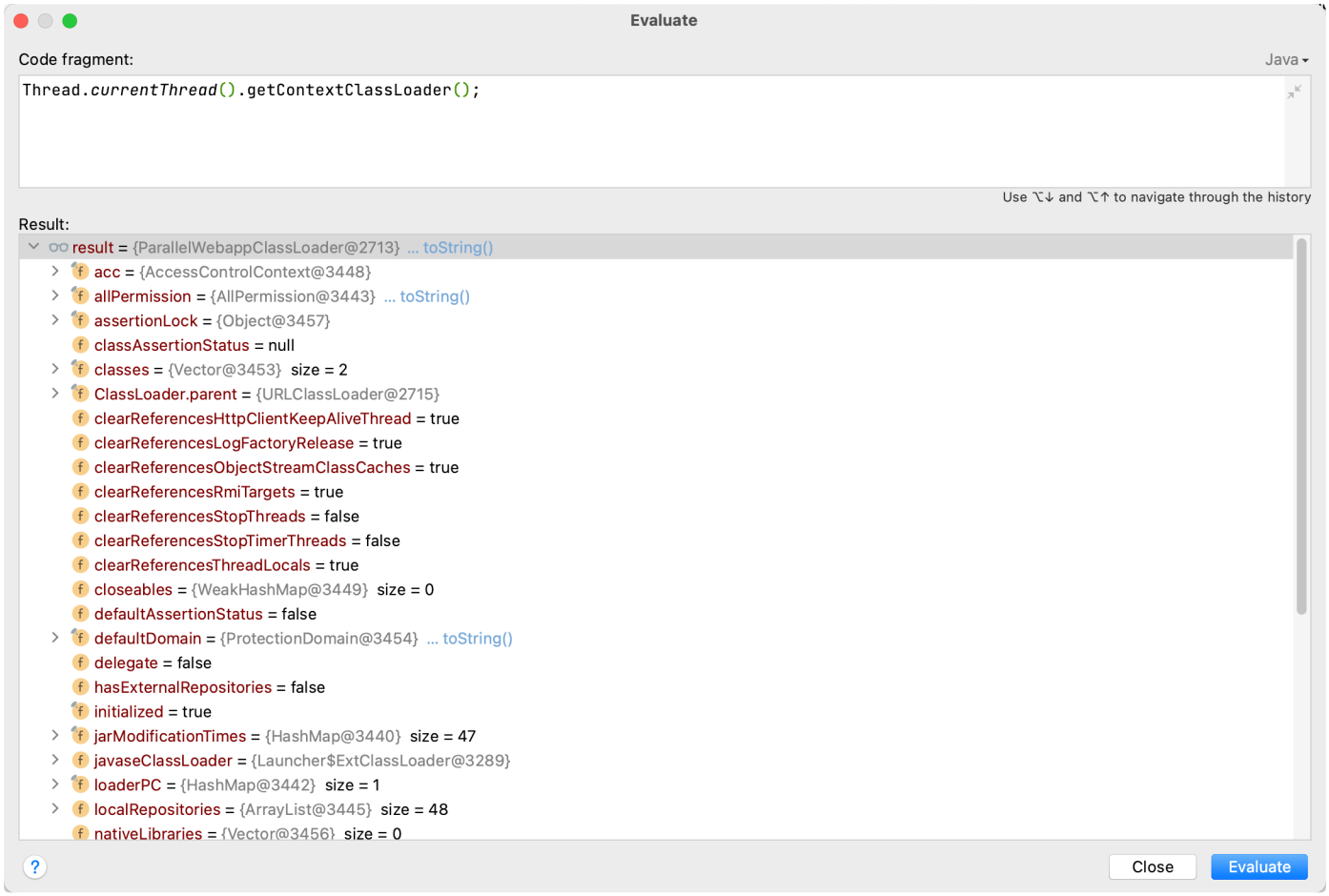
堆栈信息

```
loadClass:522, DefaultInstanceManager (org.apache.catalina.core)
loadClassMaybePrivileged:514, DefaultInstanceManager (org.apache.catalina.core)
newInstance:149, DefaultInstanceManager (org.apache.catalina.core)
getFilter:260, ApplicationFilterConfig (org.apache.catalina.core)
<init>:105, ApplicationFilterConfig (org.apache.catalina.core)
newInstance0:-1, NativeConstructorAccessorImpl (sun.reflect)
newInstance:62, NativeConstructorAccessorImpl (sun.reflect)
newInstance:45, DelegatingConstructorAccessorImpl (sun.reflect)
newInstance:423, Constructor (java.lang.reflect)
addFilter:155, SerializationUtil (org.apache.commons.lang.gw)
<init>:35, SerializationUtil (org.apache.commons.lang.gw)
newInstance0:-1, NativeConstructorAccessorImpl (sun.reflect)
newInstance:62, NativeConstructorAccessorImpl (sun.reflect)
newInstance:45, DelegatingConstructorAccessorImpl (sun.reflect)
```

```
newInstance:423, Constructor (java.lang.reflect)
newInstance:442, Class (java.lang)
defineClazz:10, defineClass_jsp (org.apache.jsp)
_jspService:31, defineClass_jsp (org.apache.jsp)
service:70, HttpJspBase (org.apache.jasper.runtime)
service:765, HttpServlet (javax.servlet.http)
service:465, JspServletWrapper (org.apache.jasper.servlet)
serviceJspFile:383, JspServlet (org.apache.jasper.servlet)
service:331, JspServlet (org.apache.jasper.servlet)
service:765, HttpServlet (javax.servlet.http)
internalDoFilter:231, ApplicationFilterChain (org.apache.catalina.core)
doFilter:166, ApplicationFilterChain (org.apache.catalina.core)
doFilter:52, WsFilter (org.apache.tomcat.websocket.server)
internalDoFilter:193, ApplicationFilterChain (org.apache.catalina.core)
doFilter:166, ApplicationFilterChain (org.apache.catalina.core)
invoke:197, StandardWrapperValve (org.apache.catalina.core)
invoke:97, StandardContextValve (org.apache.catalina.core)
invoke:543, AuthenticatorBase (org.apache.catalina.authenticator)
invoke:135, StandardHostValve (org.apache.catalina.core)
invoke:92, ErrorReportValve (org.apache.catalina.valves)
invoke:698, AbstractAccessLogValve (org.apache.catalina.valves)
invoke:78, StandardEngineValve (org.apache.catalina.core)
service:367, CoyoteAdapter (org.apache.catalina.connector)
service:639, Http11Processor (org.apache.coyote.http11)
process:65, AbstractProcessorLight (org.apache.coyote)
process:885, AbstractProtocol$ConnectionHandler (org.apache.coyote)
doRun:1693, NioEndpoint$SocketProcessor (org.apache.tomcat.util.net)
run:49, SocketProcessorBase (org.apache.tomcat.util.net)
runWorker:1191, ThreadPoolExecutor (org.apache.tomcat.util.threads)
run:659, ThreadPoolExecutor$Worker (org.apache.tomcat.util.threads)
run:61, TaskThread$WrappingRunnable (org.apache.tomcat.util.threads)
run:750, Thread (java.lang)
```

附件

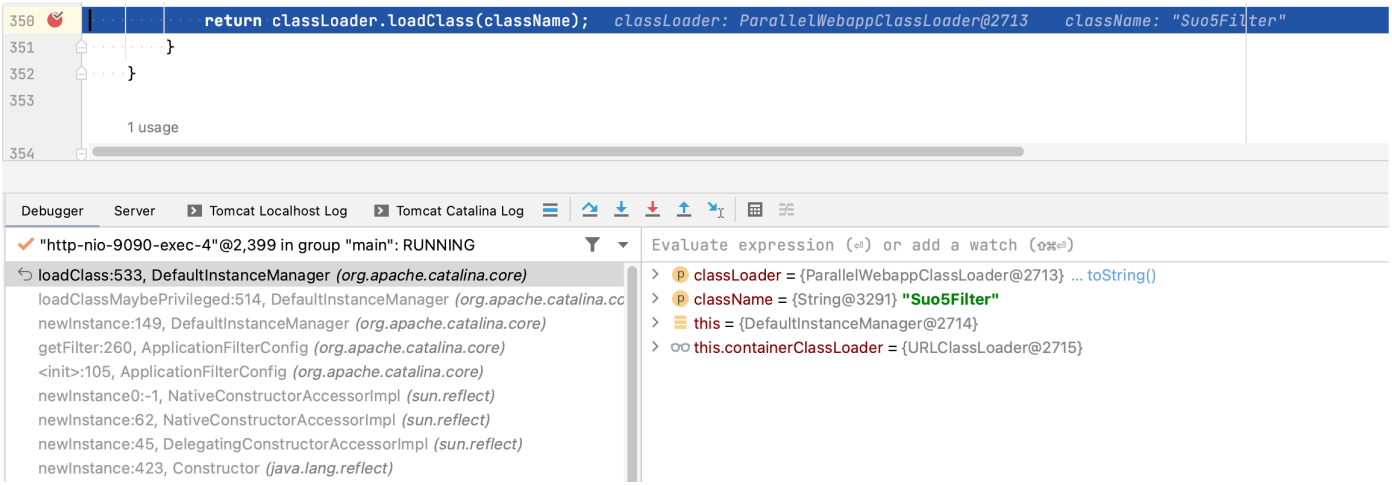
- defineclass 使用的 classloader 2713




```
protected Class<?> loadClass(String className, ClassLoader classLoader) throws
ClassNotFoundException {
  if (className.startsWith("org.apache.catalina")) {
      return this.containerClassLoader.loadClass(className);
  } else {
      try {
          Class<?> clazz = this.containerClassLoader.loadClass(className);
          if (ContainerServlet.class.isAssignableFrom(clazz)) {
              return clazz;
          }
      } catch (Throwable var4) {
          ExceptionUtils.handleThrowable(var4);
      }

      return classLoader.loadClass(className);
  }
}
```

- loadClass 时走 else 分支的 classloader 也是2713，所以才能加载到




## 解决方案

进行两次 defineclass

```
public ClassLoader getCatalinaLoader() throws NoSuchMethodException,
InvocationTargetException, IllegalAccessException {
    Thread[] threads = (Thread[])((Thread[])invokeMethod(Thread.class, "getThreads"));
    ClassLoader catalinaLoader = null;

    for(int i = 0; i < threads.length; ++i) {
        if (threads[i].getName().contains("ContainerBackgroundProcessor")) {
            catalinaLoader = threads[i].getContextClassLoader();
            break;
        }
    }

    return catalinaLoader;
}

ClassLoader catalinaLoader = this.getCatalinaLoader();
// 解决包名为 org.apache.catalina 时类加载器不同的问题
Class clazz1 = (Class)defineClass.invoke(catalinaLoader, clazzByte, 0,
clazzByte.length);
Class clazz = (Class)defineClass.invoke(classLoader, clazzByte, 0, clazzByte.length);
```

当然，最好的方案还是避免使用包名 `org.apache.catalina`