走过2013

吴建强

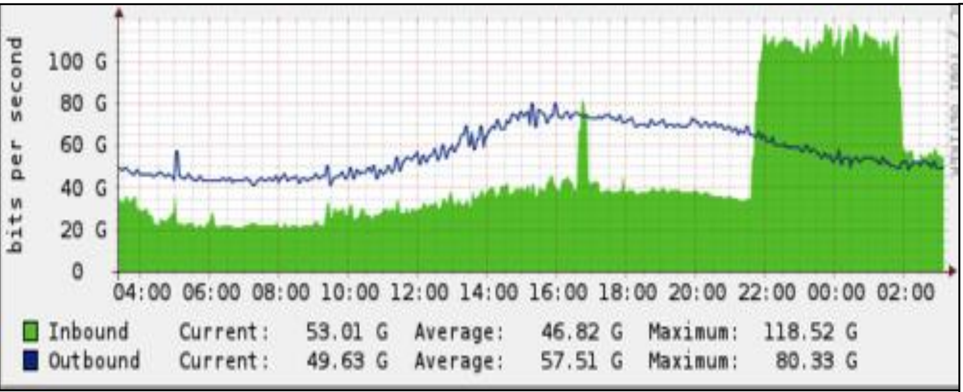
漏洞报告：bugreport@vip.sohu.com

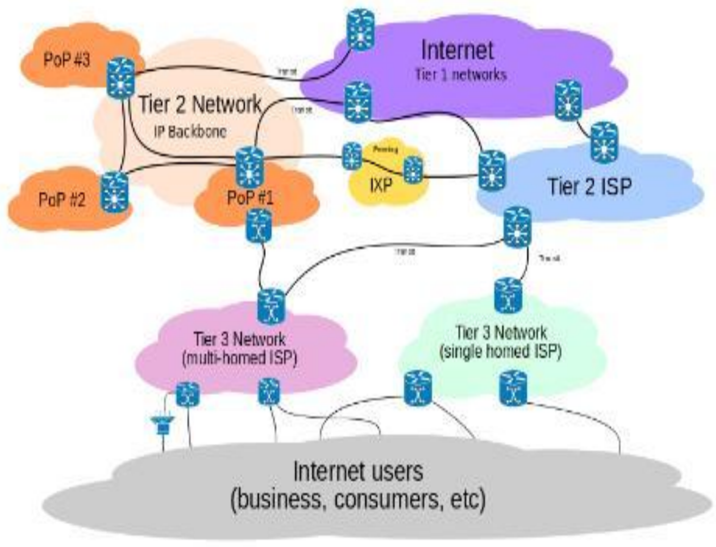
今天要讲

- DDOS
- Security as Service
- Active & Passive Web 2.0 App Scanner
- Struts2
- Iass、Paas对安全的提升
- Mobile & GSM Security

DDOS

- Spamhaus "300" G
  - 利用dns反射
  - 攻击二级提供商及网络交换中心
  - The DDoS That Almost Broke the Internet

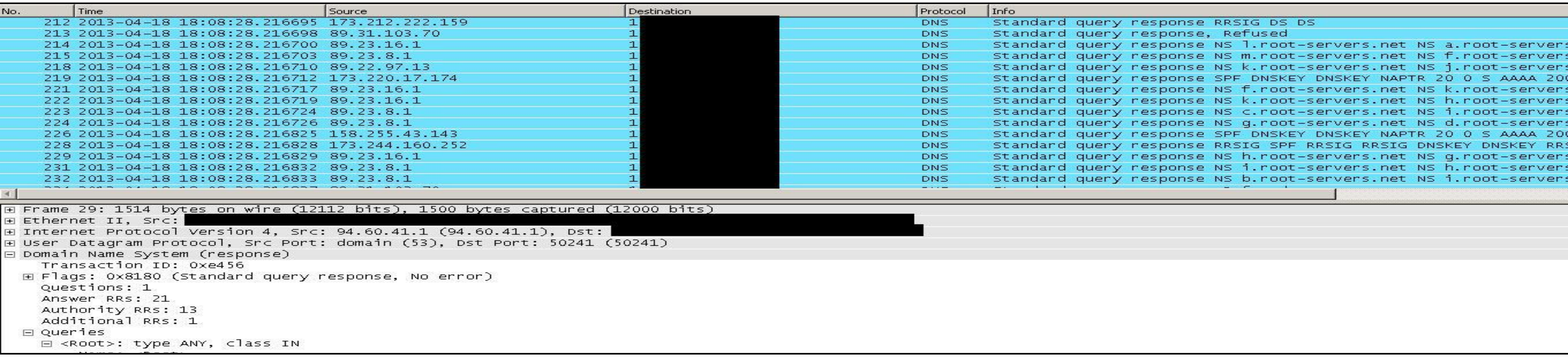




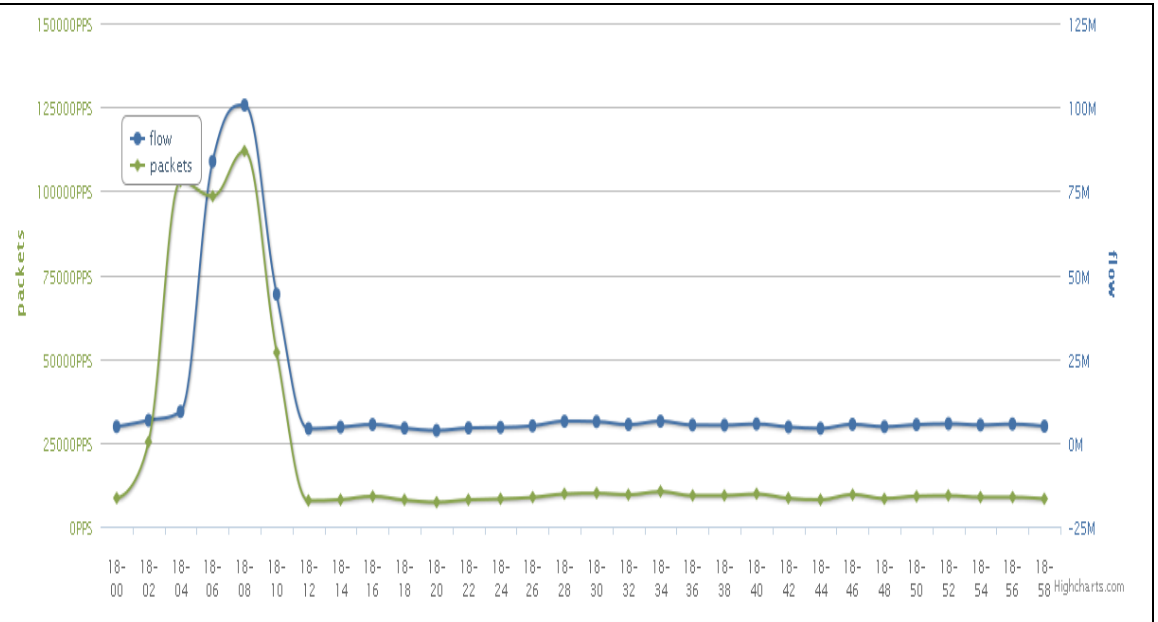
Source: wikipedia.org

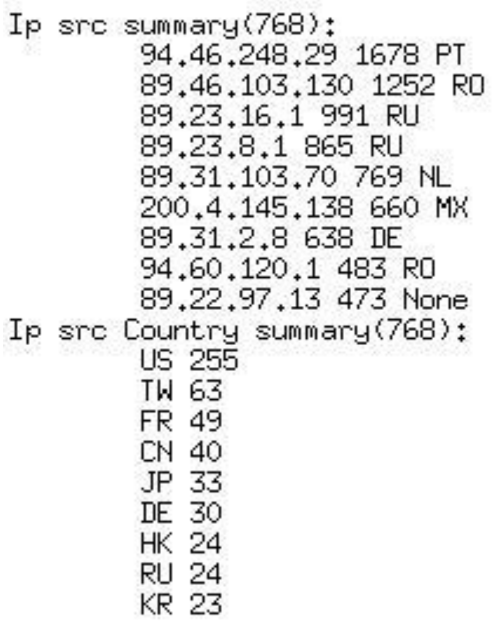
DDOS

搜狐
SOHU.com



```
No.   Time                        Source              Destination  Protocol  Info
  212 2013-04-18 18:08:28.216695  173.212.222.159     1[redacted]  DNS       Standard query response RRSIG DS DS
  213 2013-04-18 18:08:28.216698  89.31.103.70        1            DNS       Standard query response, Refused
  214 2013-04-18 18:08:28.216700  89.23.16.1          1            DNS       Standard query response NS l.root-servers.net NS a.root-servers
  215 2013-04-18 18:08:28.216703  89.23.8.1           1            DNS       Standard query response NS m.root-servers.net NS f.root-servers
  218 2013-04-18 18:08:28.216710  89.22.97.13         1            DNS       Standard query response NS k.root-servers.net NS j.root-servers
  219 2013-04-18 18:08:28.216712  173.220.17.174      1            DNS       Standard query response SPF DNSKEY DNSKEY NAPTR 20 0 S AAAA 20(
  221 2013-04-18 18:08:28.216717  89.23.16.1          1            DNS       Standard query response NS f.root-servers.net NS k.root-servers
  222 2013-04-18 18:08:28.216719  89.23.16.1          1            DNS       Standard query response NS k.root-servers.net NS h.root-servers
  223 2013-04-18 18:08:28.216724  89.23.8.1           1            DNS       Standard query response NS c.root-servers.net NS i.root-servers
  224 2013-04-18 18:08:28.216726  89.23.8.1           1            DNS       Standard query response NS g.root-servers.net NS d.root-servers
  226 2013-04-18 18:08:28.216825  158.255.43.143      1            DNS       Standard query response SPF DNSKEY DNSKEY NAPTR 20 0 S AAAA 20(
  228 2013-04-18 18:08:28.216828  173.244.160.252     1            DNS       Standard query response RRSIG SPF RRSIG RRSIG DNSKEY DNSKEY RRS
  229 2013-04-18 18:08:28.216829  89.23.16.1          1            DNS       Standard query response NS h.root-servers.net NS g.root-servers
  231 2013-04-18 18:08:28.216832  89.23.8.1           1            DNS       Standard query response NS i.root-servers.net NS h.root-servers
  232 2013-04-18 18:08:28.216833  89.23.8.1           1            DNS       Standard query response NS b.root-servers.net NS i.root-servers

⊞ Frame 29: 1514 bytes on wire (12112 bits), 1500 bytes captured (12000 bits)
⊞ Ethernet II, Src: [redacted]
⊞ Internet Protocol Version 4, Src: 94.60.41.1 (94.60.41.1), Dst:
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 50241 (50241)
⊟ Domain Name System (response)
    Transaction ID: 0xe456
  ⊞ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 21
    Authority RRs: 13
    Additional RRs: 1
  ⊟ Queries
    ⊟ <Root>: type ANY, class IN
```

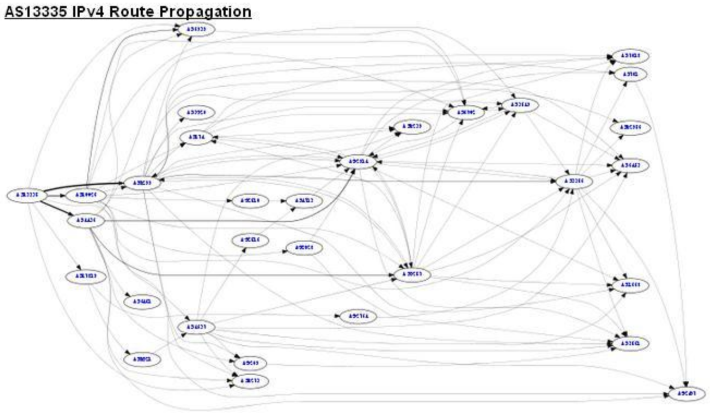


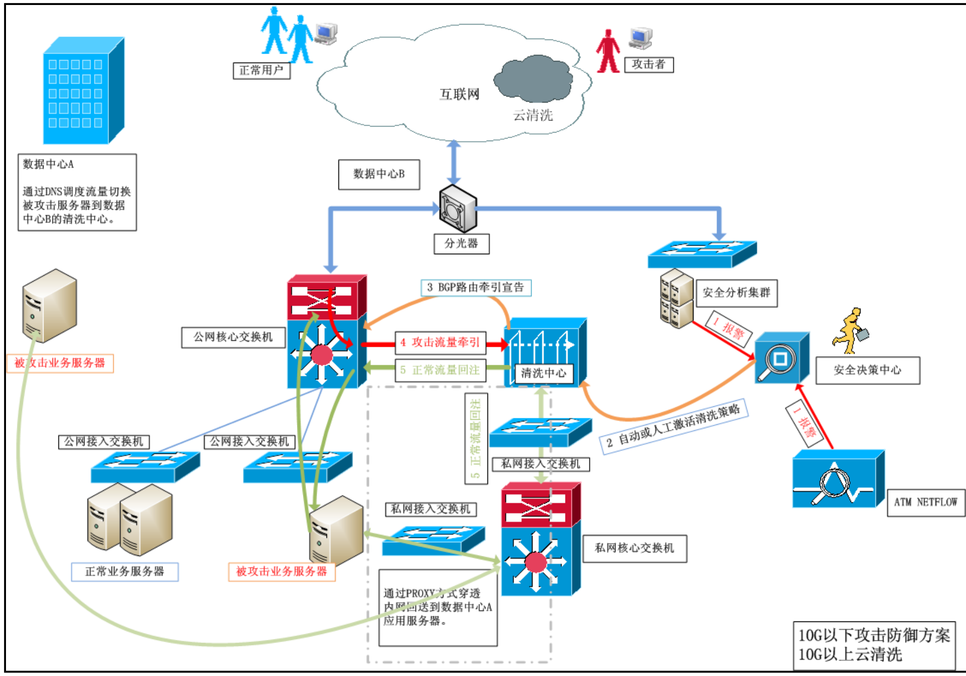


```
Ip src summary(768):
        94.46.248.29 1678 PT
        89.46.103.130 1252 RO
        89.23.16.1 991 RU
        89.23.8.1 865 RU
        89.31.103.70 769 NL
        200.4.145.138 660 MX
        89.31.2.8 638 DE
        94.60.120.1 483 RO
        89.22.97.13 473 None
Ip src Country summary(768):
        US 255
        TW 63
        FR 49
        CN 40
        JP 33
        DE 30
        HK 24
        RU 24
        KR 23
```

DDOS

- 如何解决
  - 收益分析
  - 自建清洗中心
  - anycast
  - 云清洗
  - 运营商URPF





数据中心A

通过DNS调度流量切换被攻击服务器到数据中心B的清洗中心。

通过PROXY方式穿透内网回送到数据中心A应用服务器。

10G以下攻击防御方案
10G以上云清洗

DDOS

- 打造你的“黑洞”
  - 主动牵引
    - zebra(bgp)、netfilter、nginx
  - 被动牵引
    - 在被攻击服务器实施网络层牵引

```
iptables -t nat -A PREROUTING -i eth1 -p tcp -m tcp --dport 80 -j DNAT --to-destination X.X.X.X:80
```

    - 在防护设备实施清洗后代理到被攻击服务器

Security As Service

- 输出你的价值

  En(de)crypt、Captcha

  Phish、Malware、Scanner

  Blacklist

- 降低使用难度

ACCESS_KEY = "DG74KC39ZC6BJC5312A74D7BWURW42"

SECRET_KEY = "1LCJ4f#CV6JY6pYdcXJG"

ENCRYPT_SERVICE_ENDPOINT = "https://sasp/CipherServices/encrypt"

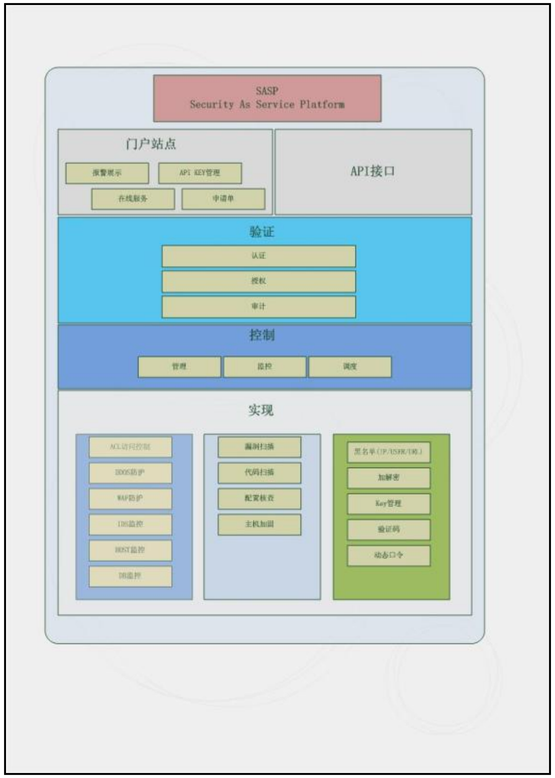
DECRYPT_SERVICE_ENDPOINT = "https://sasp/CipherServices/decrypt"

encrypt:

```
{"sign":"3fb9c19841315fe70ca54788af5b87698f91f210","status":0,"cipher":"AAAAANVsKvYbwsiK32MVSnqIYI28vYYUSXj_x5fSQmzced-R"}

 |key_version|iv|ciperdata|
```

decrypt:

```
{"sign":"ab5fde10e6607e2fbda4ed0095974894fb90d3e3","status":0,"plain":"abcdef"}
```

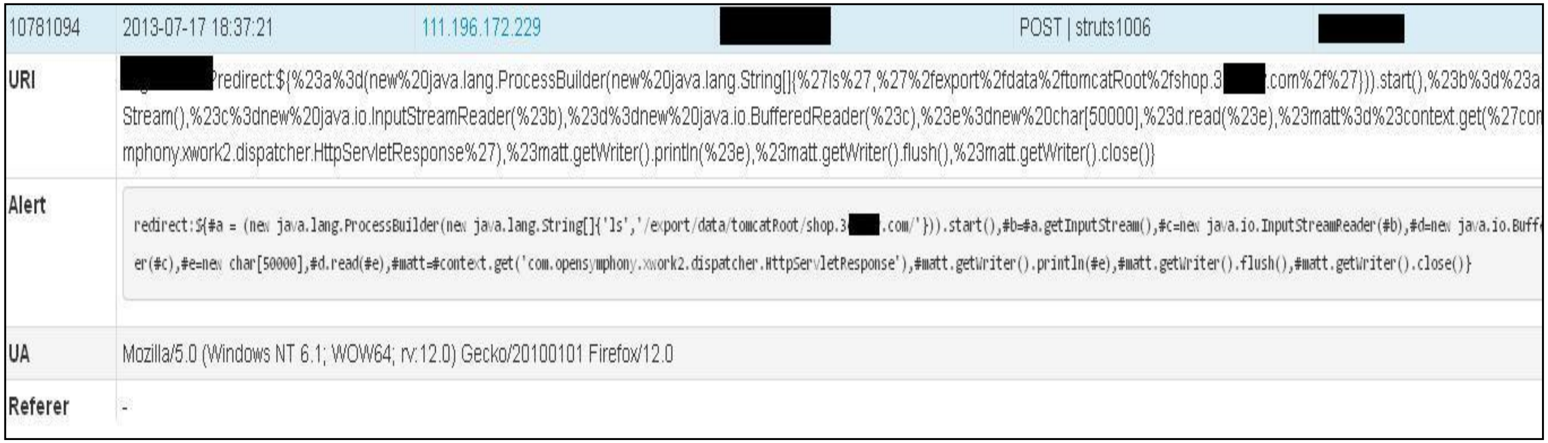


Active & Passive Web 2.0 App Scanner

- Active WEB2.0 App Scanner
  - 复杂的登陆及会话管理
  - 遍历、点击、遍历、填表、点击、onsubmit...
  - QtWebKit
- Passive Web 2.0 App Scanner
  - 基于Proxy的被动扫描
  - ...

Struts2

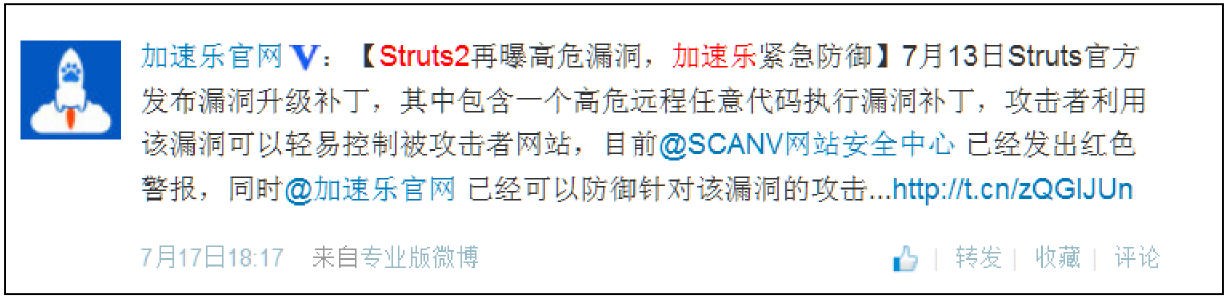
- S2-005、S2-009、S2-016
- S2-012、S2-013
    - 受限访问...
- 一个神奇的框架、一个筛子



10781094	2013-07-17 18:37:21	111.196.172.229	[redacted]	POST | struts1006	[redacted]
URI	[redacted]redirect:${%23a%3d(new%20java.lang.ProcessBuilder(new%20java.lang.String[]{%27ls%27,%27%2fexport%2fdata%2ftomcatRoot%2fshop.3[redacted].com%2f%27})).start(),%23b%3d%23a Stream(),%23c%3dnew%20java.io.InputStreamReader(%23b),%23d%3dnew%20java.io.BufferedReader(%23c),%23e%3dnew%20char[50000],%23d.read(%23e),%23matt%3d%23context.get(%27con mphony.xwork2.dispatcher.HttpServletResponse%27),%23matt.getWriter().println(%23e),%23matt.getWriter().flush(),%23matt.getWriter().close()}				
Alert	redirect:${#a = (new java.lang.ProcessBuilder(new java.lang.String[]{'ls','/export/data/tomcatRoot/shop.3[redacted].com/'})).start(),#b=#a.getInputStream(),#c=new java.io.InputStreamReader(#b),#d=new java.io.Buff er(#c),#e=new char[50000],#d.read(#e),#matt=#context.get('com.opensymphony.xwork2.dispatcher.HttpServletResponse'),#matt.getWriter().println(#e),#matt.getWriter().flush(),#matt.getWriter().close()}				
UA	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:12.0) Gecko/20100101 Firefox/12.0				
Referer	-				

Struts2

- 如果我有个灵活定义的WAF就好了
  - 商业WAF VS 开源WAF
  - 如何整合到现有的CDN、GateWay系统
  - 如：安恒明御web应用防火墙等

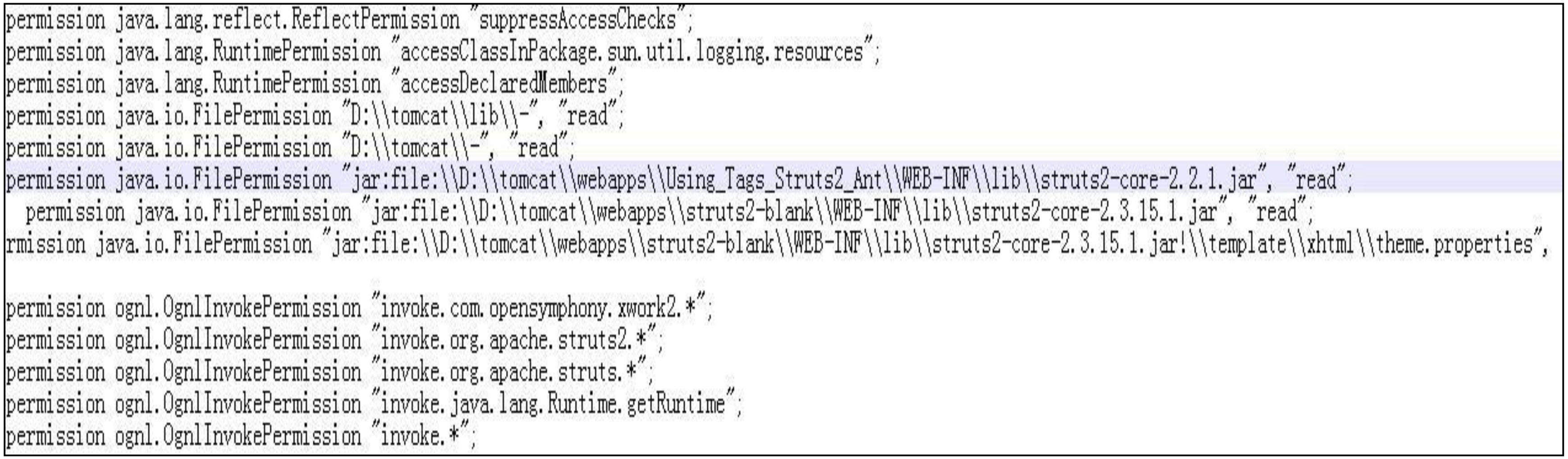


加速乐官网 V：【Struts2再曝高危漏洞，加速乐紧急防御】7月13日Struts官方发布漏洞升级补丁，其中包含一个高危远程任意代码执行漏洞补丁，攻击者利用该漏洞可以轻易控制被攻击者网站，目前@SCANV网站安全中心 已经发出红色警报，同时@加速乐官网 已经可以防御针对该漏洞的攻击...http://t.cn/zQGIJUn

7月17日18:17 来自专业版微博

Struts2

- 如果我用了Security Manager



```
permission java.lang.reflect.ReflectPermission "suppressAccessChecks";
permission java.lang.RuntimePermission "accessClassInPackage.sun.util.logging.resources";
permission java.lang.RuntimePermission "accessDeclaredMembers";
permission java.io.FilePermission "D:\\tomcat\\lib\\-", "read";
permission java.io.FilePermission "D:\\tomcat\\-", "read";
permission java.io.FilePermission "jar:file:\\D:\\tomcat\\webapps\\Using_Tags_Struts2_Ant\\WEB-INF\\lib\\struts2-core-2.2.1.jar", "read";
  permission java.io.FilePermission "jar:file:\\D:\\tomcat\\webapps\\struts2-blank\\WEB-INF\\lib\\struts2-core-2.3.15.1.jar", "read";
rmission java.io.FilePermission "jar:file:\\D:\\tomcat\\webapps\\struts2-blank\\WEB-INF\\lib\\struts2-core-2.3.15.1.jar!\\template\\xhtml\\theme.properties",

permission ognl.OgnlInvokePermission "invoke.com.opensymphony.xwork2.*";
permission ognl.OgnlInvokePermission "invoke.org.apache.struts2.*";
permission ognl.OgnlInvokePermission "invoke.org.apache.struts.*";
permission ognl.OgnlInvokePermission "invoke.java.lang.Runtime.getRuntime";
permission ognl.OgnlInvokePermission "invoke.*";
```

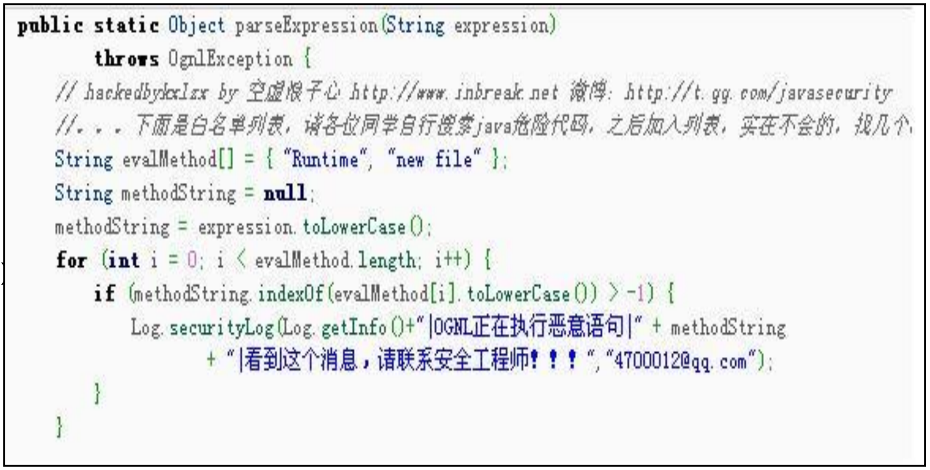
Struts2

- 如果我有自定义过补丁
  - 布置"锚"点

http://t.cn/zlnNPn6

```
public Object callMethod(Map context, Object object, String string, Object[] objects)

  throws MethodFailedException

 {

  if (object.getClass().getName().startsWith("java.")) {

      return null;

  }

 public Object callStaticMethod(Map context, Class aClass, String string, Object[] objects)

  throws MethodFailedException

 {

  return null;

 }
```

http://www.inbreak.net/?p=507

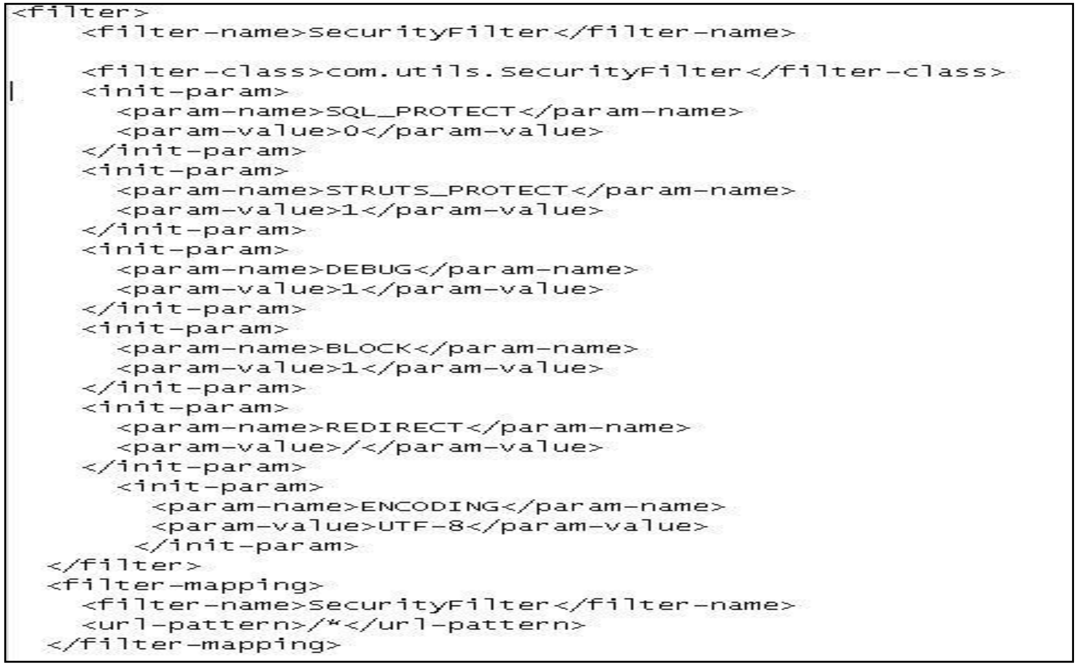


```
public static Object parseExpression(String expression)
        throws OgnlException {
    // hackedbykxlzx by 空虚浪子心 http://www.inbreak.net 微博: http://t.qq.com/javasecurity
    //. . . 下面是白名单列表，请各位同学自行搜索java危险代码，之后加入列表，实在不会的，找几个
    String evalMethod[] = { "Runtime", "new file" };
    String methodString = null;
    methodString = expression.toLowerCase();
    for (int i = 0; i < evalMethod.length; i++) {
        if (methodString.indexOf(evalMethod[i].toLowerCase()) > -1) {
            Log.securityLog(Log.getInfo()+"|OGNL正在执行恶意语句|" + methodString
                    + "|看到这个消息，请联系安全工程师！！！", "4700012@qq.com");
        }
    }
```

Struts2

- 如果我准备了一个web filter

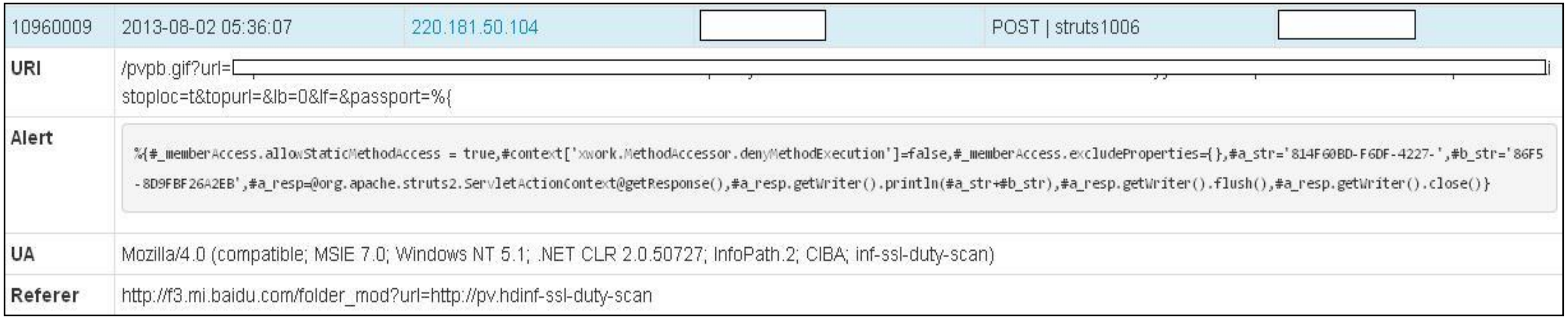
private final String[] STRUTSAttackPattern = { "StaticMethodAccess", "denyMethodExecution", "java.lang", "redirect:", "action:", "java.io", "Runtime", "context[", "#_", "org.apache.struts2" };



```
<filter>
    <filter-name>SecurityFilter</filter-name>

    <filter-class>com.utils.SecurityFilter</filter-class>
    <init-param>
      <param-name>SQL_PROTECT</param-name>
      <param-value>0</param-value>
    </init-param>
    <init-param>
      <param-name>STRUTS_PROTECT</param-name>
      <param-value>1</param-value>
    </init-param>
    <init-param>
      <param-name>DEBUG</param-name>
      <param-value>1</param-value>
    </init-param>
    <init-param>
      <param-name>BLOCK</param-name>
      <param-value>1</param-value>
    </init-param>
    <init-param>
      <param-name>REDIRECT</param-name>
      <param-value>/</param-value>
    </init-param>
      <init-param>
        <param-name>ENCODING</param-name>
        <param-value>UTF-8</param-value>
       </init-param>
  </filter>
  <filter-mapping>
    <filter-name>SecurityFilter</filter-name>
    <url-pattern>/*</url-pattern>
  </filter-mapping>
```

Struts2

- 选择并管理基础技术框架
  - 实现有充分了解？
  - 以往的漏洞类型、数量、级别？



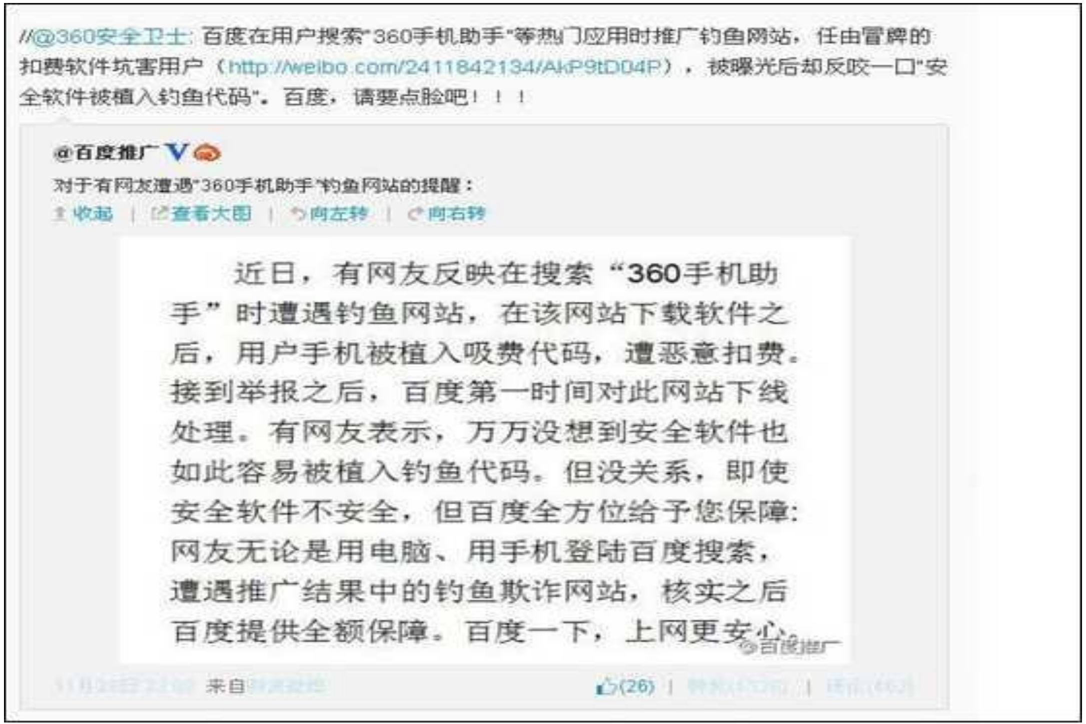
10960009	2013-08-02 05:36:07	220.181.50.104	[redacted]	POST | struts1006	[redacted]
URI	/pvpb.gif?url=[redacted]i stoploc=t&topurl=&lb=0&lf=&passport=%{				
Alert	%{#_memberAccess.allowStaticMethodAccess = true,#context['xwork.MethodAccessor.denyMethodExecution']=false,#_memberAccess.excludeProperties={},#a_str='814F60BD-F6DF-4227-',#b_str='86F5-8D9FBF26A2EB',#a_resp=@org.apache.struts2.ServletActionContext@getResponse(),#a_resp.getWriter().println(#a_str+#b_str),#a_resp.getWriter().flush(),#a_resp.getWriter().close()}				
UA	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; InfoPath.2; CIBA; inf-ssl-duty-scan)				
Referer	http://f3.mi.baidu.com/folder_mod?url=http://pv.hdinf-ssl-duty-scan				

Iass、Paas对安全的提升

- IAAS
  - 可定义的安全镜像
  - 灵活的升级机制
  - 强制访问控制措施
- PAAS(java)
  - 统一的Security Policy
  - Javaagent、instrument
  - 代码热替换

Mobile & GSM Security

- Andiod Security
  - Webview
  - Uncovering Android Master Key



//@360安全卫士: 百度在用户搜索"360手机助手"等热门应用时推广钓鱼网站，任由冒牌的扣费软件坑害用户（http://weibo.com/2411842134/AkP9tD04P），被曝光后却反咬一口"安全软件被植入钓鱼代码"。百度，请要点脸吧！！！

@百度推广

对于有网友遭遇"360手机助手"钓鱼网站的提醒：

近日，有网友反映在搜索“360手机助手”时遭遇钓鱼网站，在该网站下载软件之后，用户手机被植入吸费代码，遭恶意扣费。接到举报之后，百度第一时间对此网站下线处理。有网友表示，万万没想到安全软件也如此容易被植入钓鱼代码。但没关系，即使安全软件不安全，但百度全方位给予您保障：网友无论是用电脑、用手机登陆百度搜索，遭遇推广结果中的钓鱼欺诈网站，核实之后百度提供全额保障。百度一下，上网更安心。

Mobile & GSM Security

- 伪基站
- 短信监听
- 基于手机号的用户名认证方式

感谢

- 协助搜狐改进产品安全的研究者及厂商
- 业界同仁的分享
- 同事的努力

漏洞报告：bugreport@vip.sohu.com