

最后一道防线，主机端的威胁感知体系

椒图科技 李栋



目录 Index

- 威胁情报在终端落地的挑战
- 威胁情报从获取到落地时间差带来的潜在危害
- 主机自身的威胁感知体系:从应急响应到持续响应
- 主机威胁感知体系建设的挑战

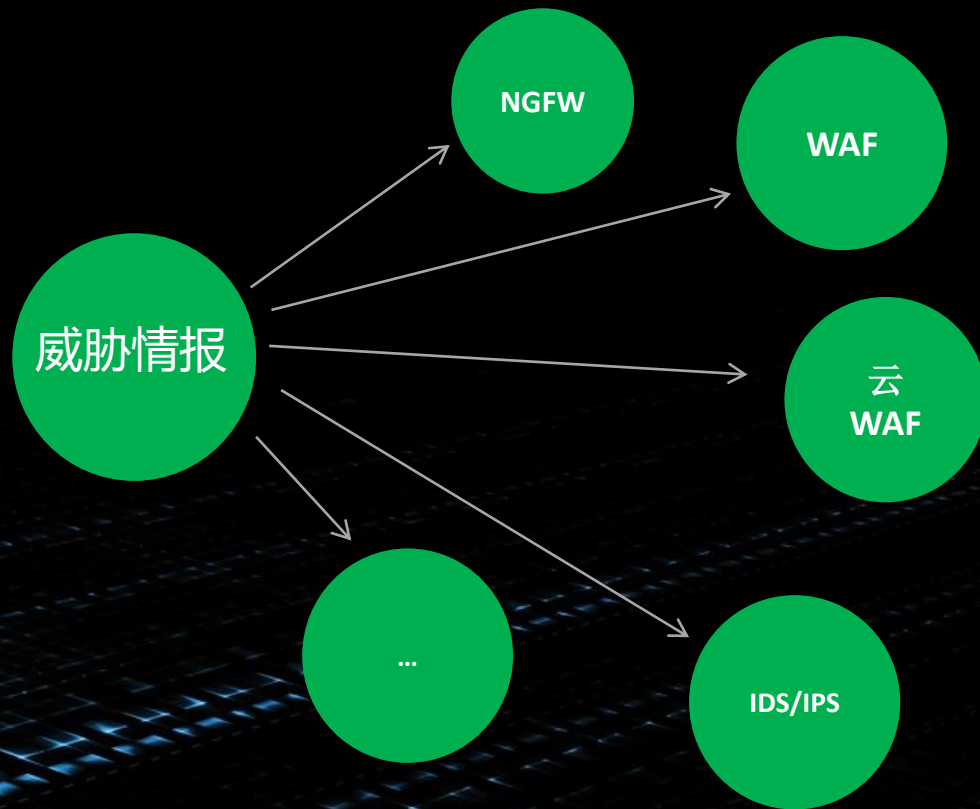
威胁情报落地面临的挑战

- 威胁情报来源：真实性、有效性、实时性
- 数据整合与降噪
- 在终端落地

终端可用的威胁情报

- IP地址黑名单
- 病毒特征码
- Webshell
- 系统/应用安全漏洞

威胁情报落地





ATTACK FREE

威胁情报从获取到落地的时间差，给黑客创造Attack free机会

案例：2017年03月07日 Struts2 漏洞CVE编号CVE-2017-5638

漏洞披露时间：2017-03-07

漏洞编号

CVE-2017-5638

漏洞简介

Struts使用的Jakarta解析文件上传请求包不当，当远程攻击者构造恶意的Content-Type，可能导致远程命令执行。

实际上在default.properties文件中，struts.multipart.parser的值有两个选择，分别是jakarta和pell（另外原本其实也有第三种选择cos）。其中的jakarta解析器是Struts 2框架的标准组成部分。默认情况下jakarta是启用的，所以该漏洞的严重性需要得到正视。

影响范围

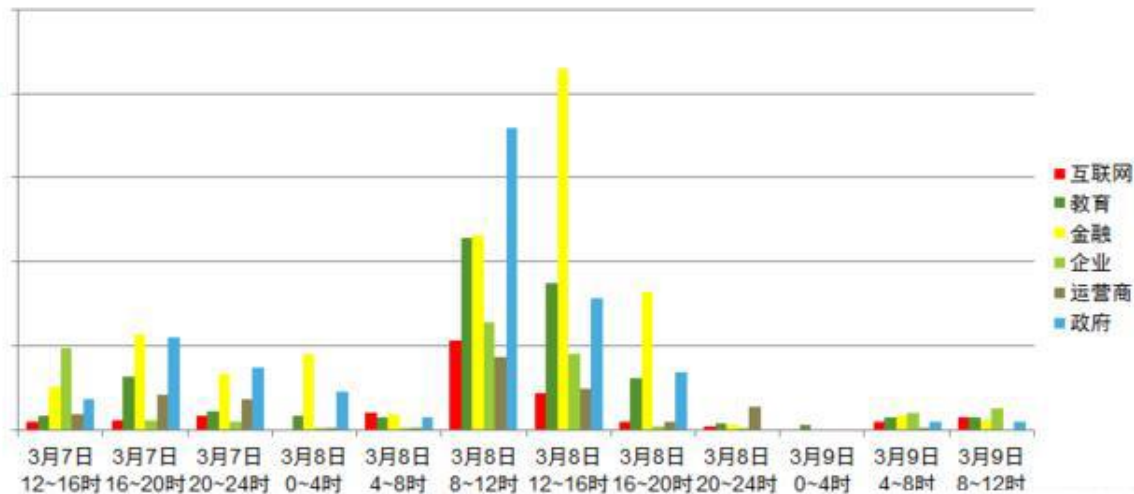
Struts 2.3.5 – Struts 2.3.31

Struts 2.5 – Struts 2.5.10

案例：2017年03月07日 Struts2 漏洞CVE编号CVE-2017-5638

客户检测并修复struts漏洞时间轴，截止3月9日，仍有部分用户没有修复漏洞或更新规则

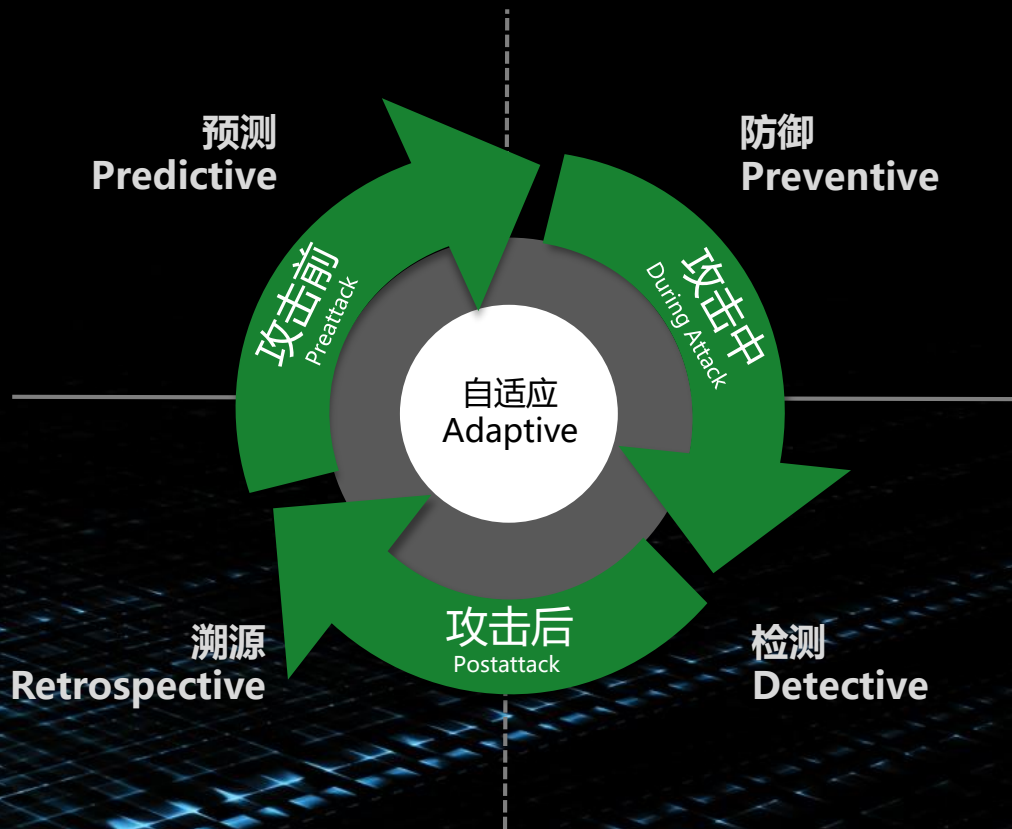
Struts2漏洞各行业检测积极性



ATTACK FREE

威胁情报从获取到落地之前，主机端的威胁感知及防御体系

主机端威胁感知体系的建设要求



From gartner

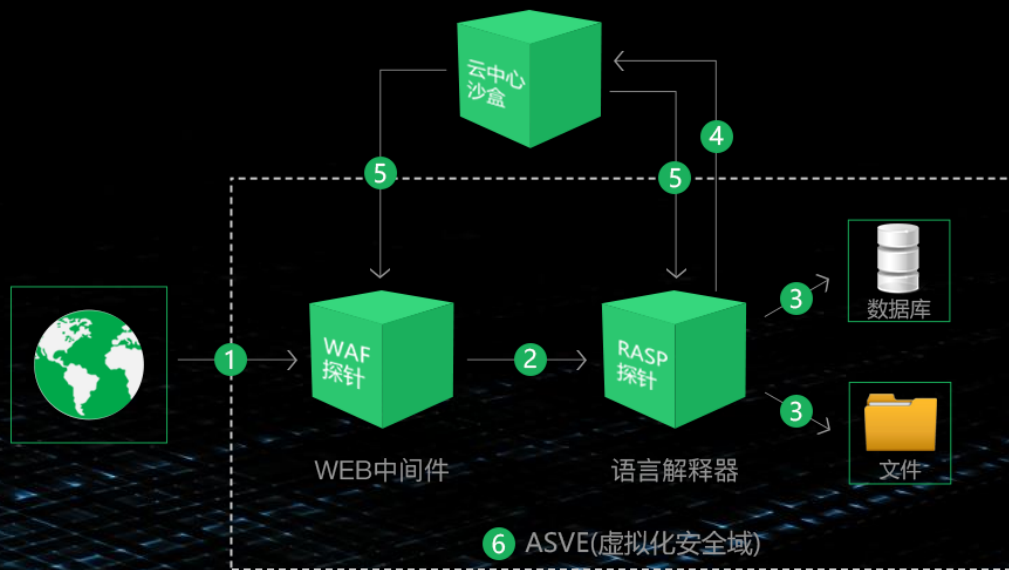
1. “预测能力”使安全系统可从外部监控下的黑客行动中学习，以主动锁定对现有系统和信息具有威胁的新型攻击，并对漏洞划定优先级和定位。该情报将反馈到预防和检测功能，从而构成整个处理流程的闭环。
2. “防御能力”是指一系列策略集、产品和服务可以用于防御攻击。这个方面的关键目标是通过减少被攻击面来提升攻击门槛，并在受影响前拦截攻击动作。
3. “检测能力”用于发现那些逃过防御网络的攻击，该方面的关键目标是降低威胁造成的“停摆时间”以及其他潜在的损失。检测能力非常关键，因为企业应该假设自己已处在被攻击状态中。
4. “回溯能力”用于高效调查和补救被检测分析功能(或外部服务)查出的事务，以提供入侵认证和攻击来源分析，并产生新的预防手段来避免未来事故。

我们对主机端威胁感知体系的理解

- 符合Gartner标准
- 足够智能，用程序取代人工
- 动态防御，从应急响应到持续响应

主机端的威胁感知体系建设实践：从应急响应到持续响应

■ WAF探针+RASP探针+沙盒



- 1** 网络流量在经过web中间件（IIS、apache、nginx、tomcat等）时首先会经过WAF探针的过滤，通过防护规则（基于签名）可以有效的防御已知安全漏洞攻击，用户也可以自定义防护规则。
- 2** 网络流量到达语言解释器，云锁RASP探针会再次对应用系统的流量、上下文、行为进行持续监控，识别及防御已知及未知威胁，能有效防御SQL注入、命令执行、文件上传、任意文件读写、反序列化、Struts2等基于传统签名方式无法有效防护的应用漏洞；
- 3** 通过双重检测的流量才可以访问数据库或者文件。
- 4** 检测有异常行为的webshell，云锁会将样本上传回云中心沙盒，基于脚本虚拟机的无签名Webshell检测技术，可以有效检测各种加密、变形的Webshell。
- 5** 云锁独创虚拟化安全域技术（ASVE），通过将应用进程放入虚拟化安全域内，限制应用进程权限，防止黑客利用应用程序漏洞提权、创建可执行文件等非法操作
- 6** 沙盒将检测结果返回WAF探针和RASP探针，并自动更新防护规则。

主机端的威胁感知体系

■ WEB中间件WAF探针

在web中间件中插入过滤插件（WAF探针）的方式，通过多维度防护规则可以有效的防御已知安全漏洞攻击，也支持用户自定义规则和对接威胁情报。

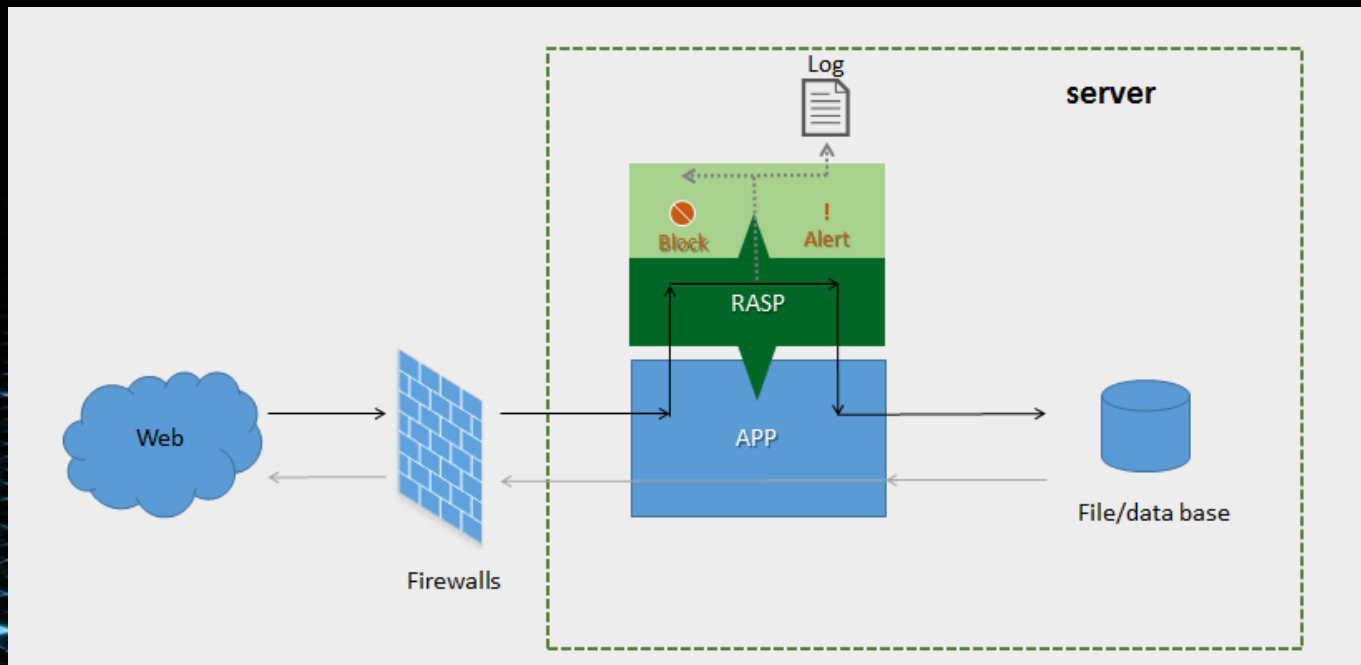


- 防护能力
 - ✓ 常见网络攻击（SQL注入、XSS、溢出攻击等）
 - ✓ CC攻击(独创session验证模式，高效验证正常访问/机器攻击)
- 对接威胁情报
 - ✓ 每天1500W+ 攻击记录
 - ✓ 4000W+ IP 信誉库
 - ✓ 海量 webshell样本（已知、新捕获）
 - ✓ 第三方威胁情报平台数据

主机端的威胁感知体系

■ RASP(Runtime Application Self Protection)

对于穿过WAF探针的流量，RASP探针会进行第二次检测，对应用系统的流量、上下文、行为进行持续监控，识别及防御已知及未知威胁。能有效防御SQL注入、命令执行、文件上传、任意文件读写、反序列化、Struts2等基于传统签名方式无法有效防护的应用漏洞。



RASP防护能力

- SQL注入
- 命令执行
- 文件上传
- 反序列化
- 任意文件读写
- 文件包含
- Struts2
- Webshell
- 网站后台
- CC攻击
- XSS攻击
- 中间件漏洞
- 敏感词过滤
- 网站防盗链
- WEB中间件溢出攻击

RASP与WAF对比

RASP	WAF
极高的覆盖度和兼容多种协议	Http协议
保护更全面	仅监控用户输入
误报率低	误报率较高
风险点定位更快速、更准确	无法快速、准确的定位风险点
不依赖网络边界	依赖网络边界
动态基于行为:可检测未知威胁	静态基于规则：只能防御已知威胁

1000

■ 沙箱 (sandbox)


基于脚本虚拟机（沙盒）的无签名Webshell检测技术，有效检测各种加密、变形的Webshell基于异常行为的检测技术，可有效检测出未知威胁。通过在内核及应用层探针中设置监控点，持续对系统的行为进行学习，可有效检测出系统中存在的异常行为，并在综合判定后产生告警。

■ 脚本虚拟机的优势

- 不依赖文本特征检测
- 可检测自加密的脚本
- 可检测未活动的WebShell
- 支持php asp .net java 编写的webshell



沙盒捕获未知webshell实例



安全无“锁”不在

总览

边界管理

服务器管理

网站管理

事件管理

事件列表

日志查询

告警设置

账户管理

子账户管理

2017-7-14 星期五

云锁年中大促，安全与优惠同行，点击进入

yunsuo-1115 退出

云锁 > 事件管理 > 事件列表

批量处理

选择服务器

发现未知Webshell

IP关键字或类型

Q 查询

<input type="checkbox"/>	攻击时间	事件类型	事件摘要	服务器	风险等级	操作	状态
<input type="checkbox"/>	2017-07-12 13:31:31	发现未知Webshell	103.22.200.190 (日本) 通过 www.yewn....		高危	查看报告	未处理
<input type="checkbox"/>	2017-07-12 13:29:41	发现未知Webshell	103.22.200.190 (日本) 通过 未知Websh...		高危	查看报告	未处理
<input type="checkbox"/>	2017-07-09 19:24:04	发现未知Webshell	23.225.200.144 (美国) 访问 未知Websh...		高危	查看报告	未处理
<input type="checkbox"/>	2017-07-04 15:39:37	发现未知Webshell	23.225.200.144 (美国) 访问 未知Websh...		高危	查看报告	未处理
<input type="checkbox"/>	2017-07-03 16:19:54	发现未知Webshell	36.251.85.191 (中国福建福州) 访问 未...		高危	查看报告	未处理
<input type="checkbox"/>	2017-07-03 16:19:35	发现未知Webshell	36.251.85.191 (中国福建福州) 访问 未...		高危	查看报告	未处理
<input type="checkbox"/>	2017-06-19 14:02:37	发现未知Webshell	192.168.1.4 (局域网) 访问 未知Webshel...	192.168.9.133	高危	查看报告	未处理
<input type="checkbox"/>	2017-06-19 13:22:56	发现未知Webshell	192.168.1.4 (局域网) 访问 未知Webshel...	192.168.9.133	高危	查看报告	未处理
<input type="checkbox"/>	2017-06-19 11:01:45	发现未知Webshell	192.168.1.4 (局域网) 访问 未知Webshel...	192.168.9.133	高危	查看报告	未处理
<input type="checkbox"/>	2017-06-16 18:25:57	发现未知Webshell	192.168.1.118 (局域网) 访问 未知Webs...	192.168.9.133	高危	查看报告	未处理

共计查询 93 条记录，当前 1 页 / 10 页

首页

上一页

下一页

尾页



沙盒捕获未知webshell实例

攻击追溯



点我咨询

TOP

沙盒捕获未知webshell实例

IOC

23.225.200.144 (美国) 访问 未知Webshell www.zjlongre.org/include/sitemap.class.php (物理路

径: /home/wwwroot/www_zjlongre_org/public_html/include/sitemap.class.php) 已拦截

域名请求: http://www.zjlongre.org/include/sitemap.class.php

请求方法: POST

请求参数: z0=NzU1MTE5O08pbmlfc2V0KCJkaXNwbGF5X2Vycm9ycylsjaiktAc2V0X3RpbWVfbGltXQoMcK7QHNIldF9tYWdpY19xdW90ZXNfcuVudGltZSgwKTtY2hvKCItPnwiKTs.....

操作类型: 执行命令

操作扩展: runtime-created function



IP: 23.225.200.144

地址: 美国

网络流量



应用

用户: www

类型: web

进程路径: /www/wdlinux/httpd-2.2.22/bin/httpd

页面路径: /home/wwwroot/www_zjlongre_org/public_html/include/sitemap.class.php

下载

操作



操作对象

执行命令: function __lambda_func() { @eval(base64_decode("QGv2YwwoJF9QT1NU....")); }



点我咨询

TOP

攻击追溯

挑战

建设主机端威胁感知体系，那些年我们走过的坑

高可用性

High usaability

■ 如何保证高可用性？

- 全面支持公有云、私有云、混合云，跨系统版本、物理架构管理
- 减少资源占用 -- 内存占用25-50M之间
- 业务优先原则
- 不依赖系统的iptables、selinux、syslog、weblog等



主环境兼容性

Environment fitness

■ 环境兼容性

■ 操作系统版本支持：

- ✓ Windows Server 2003 SP2 (x86/x64) 、 Windows Server 2008 (x86/x64) 、 Windows Server 2012
- ✓ Linux内核版本支持：280+
- ✓ RedHat 4.3~RedHat 5.11 (x86/x64) 、 RedHat 6.0~RedHat 6.7 (x86/x64) 、 RedHat 7.0~RedHat 7.2
- ✓ CentOS 4.3~CentOS 5.11 (x86/x64) 、 CentOS 6.0~CentOS 6.7 (x86/x64) 、 CentOS 7.0~CentOS 7.2
- ✓ Ubuntu10.0以上
- ✓ Suse 10~Suse 10 sp3、 Suse 11~Suse 11 sp3、 Suse 12
- ✓ 中标麒麟
- ✓ 红旗Redflag3~4

■ web中间件支持：

- ✓ IIS 6/IIS 7/IIS 7.5/IIS 8
- ✓ Apache 2.0/Apache 2.2/Apache 2.4 (x86、 x64)
- ✓ Nginx 1.0.*、 Nginx 1.2.*、 Nginx 1.4.*、 Nginx 1.6.*~Nginx 1.11.*
- ✓ kangle
- ✓ Tomcat、 Weblogic、 WebSphere、 TongWeb、 Jboss、 Glassfish、 Jetty等

■ 主机控制面板支持：

- ✓ Wdcp/AMH/Cpanel/zpanel/virtualmin/lumanager/LNMP/宝塔/一对一/星外等





椒图科技 李栋