第四届全国网络与信息安全防护峰会

安全威胁情报体系建设实践

胡珀(lake2)

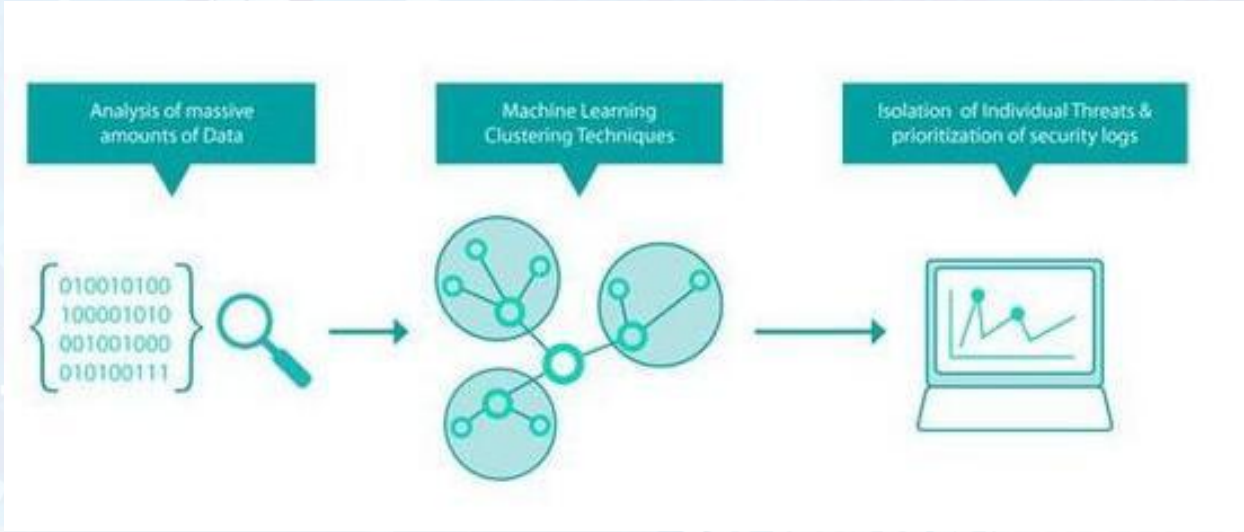
腾讯 · 安全平台部

关于我

胡珀 ， lake2 ， lakehu

- 腾讯T4安全专家，目前负责腾讯的应用安全和运维安全
- 2007年加入**腾讯**，一直在**安全平台部**从事安全工作
- 安全事件响应、渗透测试、安全培训、安全评估、安全规范、系统建设
- 腾讯安全应急响应中心（TSRC）与**威胁情报奖励计划**
- 移动安全 & 智能设备安全

什么是威胁情报



大概理解为通过**数据分析**发现的**异常线索**

一个切身体会——安全事件爆发过程

事件发生 -> 地下流传 -> 事件爆发

CSDN详解600万用户密码泄露始末：暂关闭登录

2011年12月21日22:07　腾讯科技[微博]　我要评论(0)　字号： T | T

腾讯科技讯 北京时间12月21日晚间消息，中国开发者技术在线社区CSDN今晚发表声明，就“600万用户账号密码泄露”一事公开道歉，承认部分用户账号面临风险，将临时关闭用户登录，并要求“2009年4月以前注册的帐号，且2010年9月之后没有修改过密码”的用户立即修改密码。

CSDN今日证实600万数据库泄漏，已向公安机关报案，公安机关也正在调查相关线索。

据了解，今日腾讯微博网友爆料，黑客在网上公开了CSDN用户数据库，涉及到的账户总量高达600万个，此次CSDN泄漏的密码无任何加密明文形式。由于CSDN用户多为程序员，此次事件影响巨大。

以下为声明全文：

尊敬的CSDN会员：

我们非常抱歉，近日发生了CSDN用户数据库泄露事件，您的用户密码可能被公开。我们恳切地请您修改CSDN相关密码，如果您在其他网站也使用同一密码。请一定同时修改相关网站的密码。

论威胁情报对企业信息安全的重要性

简单说就是威胁情报可以帮助企业**提前感知风险**，在事件爆发前**及时规避**

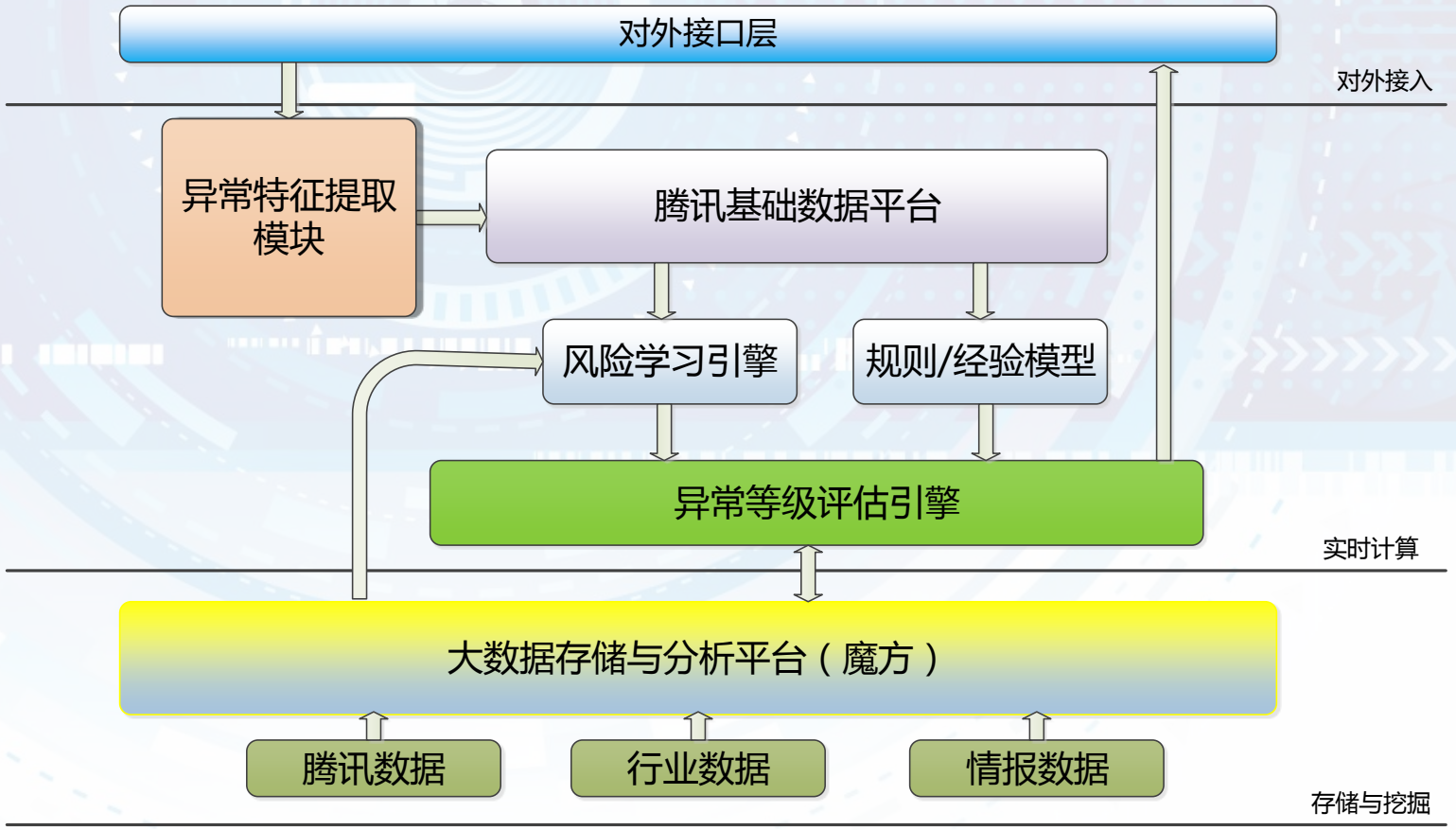
论威胁情报对安全产品的重要性

简单说就是威胁情报可以帮助安全产品**提升核心竞争力**

分析、交换、截取

产品的威胁情报应用

实践：腾讯的安全大数据分析框架



安全系统调用

大数据分析

安全系统　　情报交换　　情报团队

实践：威胁情报奖励计划

奖励内容由**安全漏洞**扩展为**威胁情报**

[TPSA15-20] 关于 “威胁情报奖励计划（试行）” 启动的

公告编号：TPSA15-20
公告来源：TSRC
发布日期：2015-10-15
公告内容：

腾讯安全应急响应中心（简称TSRC）于2012年5月启动了，在三年多的不断试错和改进中，得到了业界广大安
提高了腾讯产品和业务的安全级别。但我们仍然觉得做得还不够，我们希望再来点改进。

自即日起，TSRC原有的“**安全漏洞奖励计划**”正式升级为“**威胁情报奖励计划**”——TSRC除原有的收集腾讯安
关的任何安全威胁情报，一经确认，即按照威胁情报评分危害级别给予奖励。

【适用条件】

1）腾讯的产品和业务漏洞相关的安全情报，包括但不限于漏洞线索、攻击线索、攻击者相关信息、攻击方式、
2）通过TSRC平台提交并经过TSRC工作人员确认有效，且为首个相关情报提交者；
3）情报未报告给其他机构或组织

此链接可无需授权访问漏洞详情，请严格保密！

漏洞名称：利用代码非法改密码[redacted]
提交时间：2015-11-15 09:19:23
漏洞类型：号码安全 ▾ 盗号 ▾
危害等级：高 ▾
贡 献 值：[redacted] (评分标准)　安全币：[redacted]
处理进展

提交漏洞 — 审核中 — 已确认 — 已修复 — 已复查

漏洞详情：

一、详细说明：昨天晚上有人利用代码直接改无密码保护的[redacted]号码，改完还直接设置密保手机

二、漏洞证明：
343[redacted]，117[redacted]1，833[redacted]们可以查这几个号的记录，绝对不是正常改密和设置密保手机

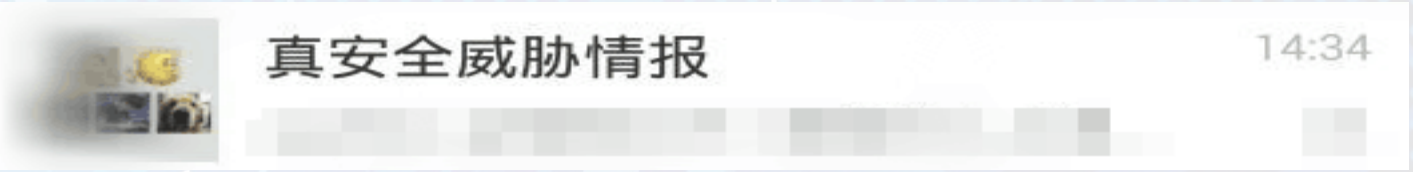
三、修复方案：

状态变更详情

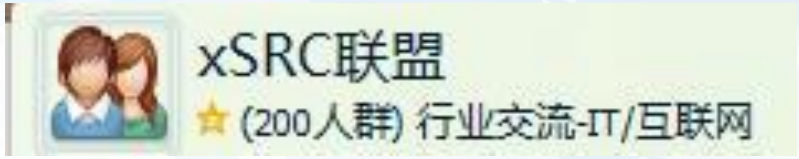
处理时间	处理信息
2015-11-15 09:19:24	用户[redacted]报告了该漏洞。
2015-11-15 10:59:02	感谢您的反馈，问题评估中，我们可能会联系您以获得您的协助。(xcx33@TSRC)
2015-11-15 18:07:39	非常感谢您的报告，问题已确认，修复中。(qwerty@TSRC)

用户提供线索，TSRC核实后按照威胁情报奖励计划给予高风险奖励

实践：情报共享联盟

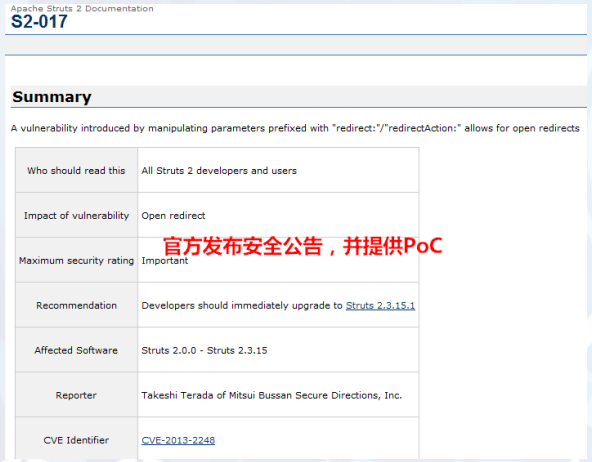


BAT3W 个人的安全威胁情报共享群



xSRC共享群

应用实例：struts2 命令执行漏洞（S2-017）


Apache Struts 2 Documentation

S2-017

Summary

A vulnerability introduced by manipulating parameters prefixed with "redirect:"/"redirectAction:" allows for open redirects

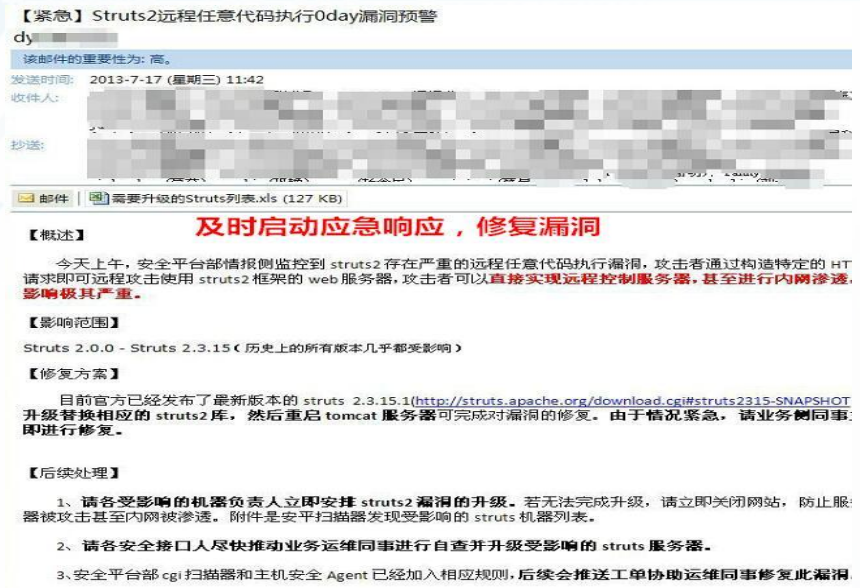
Who should read this	All Struts 2 developers and users
Impact of vulnerability	Open redirect
Maximum security rating	Important
Recommendation	Developers should immediately upgrade to Struts 2.3.15.1
Affected Software	Struts 2.0.0 - Struts 2.3.15
Reporter	Takeshi Terada of Mitsui Bussan Secure Directions, Inc.
CVE Identifier	CVE-2013-2248

官方发布安全公告，并提供PoC

白帽子上报漏洞到TSRC

漏洞发生 → 地下流传 → 情报获悉 → 应急响应 → 漏洞爆发

白帽子根据PoC调试出exp


【紧急】Struts2远程任意代码执行0day漏洞预警

该邮件的重要性为: 高。

发送时间: 2013-7-17 (星期三) 11:42

收件人:

抄送:

邮件 | 需要升级的Struts列表.xls (127 KB)

及时启动应急响应，修复漏洞

【概述】

今天上午，安全平台部情报侧监控到 struts2 存在严重的远程任意代码执行漏洞，攻击者通过构造特定的 HT 请求即可远程攻击使用 struts2 框架的 web 服务器，攻击者可以直接实现远程控制服务器，甚至进行内网渗透，影响极其严重。

【影响范围】

Struts 2.0.0 - Struts 2.3.15（历史上的所有版本几乎都受影响）

【修复方案】

目前官方已经发布了最新版本的 struts 2.3.15.1(http://struts.apache.org/download.cgi#struts2315-SNAPSHOT 升级替换相应的 struts2 库，然后重启 tomcat 服务器可完成对漏洞的修复。由于情况紧急，请业务侧同事即进行修复。

【后续处理】

1、请各受影响的机器负责人立即安排 struts2 漏洞的升级。若无法完成升级，请立即关闭网站，防止服器被攻击甚至内网被渗透。附件是安平扫描器发现受影响的 struts 机器列表。

2、请各安全接口人尽快推动业务运维同事进行自查并升级受影响的 struts 服务器。

3、安全平台部 cgi 扫描器和主机安全 Agent 已经加入相应规则，后续会推送工单协助运维同事修复此漏洞

应用实例：XCodeGhost事件

关于使用非苹果官方XCODE存在植入恶意代码情况的预警通报

来源：CNCERT　时间：2015-09-14

近日，CNCERT监测发现，开发者使用非苹果公司官方渠道的XCODE工具开发苹果应用程序（苹果APP）时，会向正常的苹果APP中植入恶意代码。被植入恶意程序的苹果APP可以在App Store正常下载并安装使用。该恶意代码具有信息窃取行为，并具有进行恶意远程控制的功能。

目前，CNCERT正在加强分析，并将此预警信息通报相关开发者或互联网企业，在开发苹果APP过程中，切勿使用非苹果官方渠道的XCODE工具，以维护广大用户的个人信息安全。

分析发现XCodeGhost病毒

上报CNCERT
通知Apple

异常分析 → 情报发现 → 应急响应 → 情报共享 → 事件爆发

发现异常

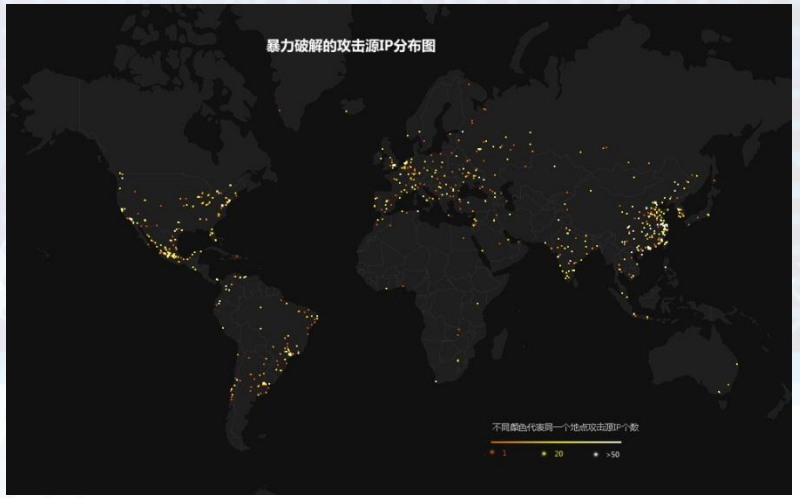
新版本APP发布

低调处理过程中事件爆发

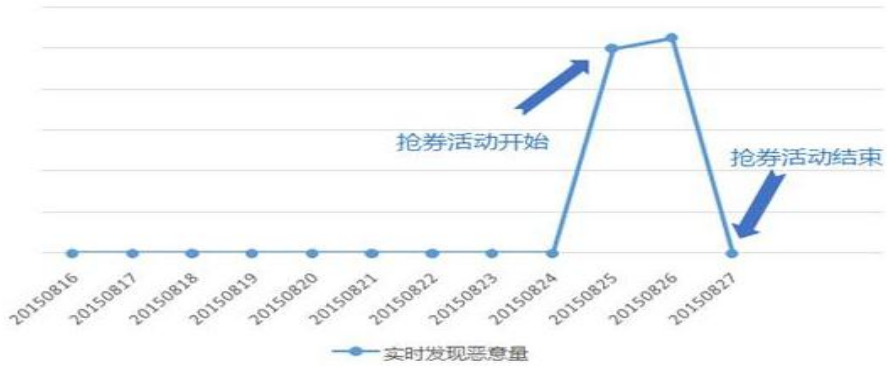
应用实例：IP信誉库的应用

CC攻击防护	• 白IP放过 • 灰&黑IP下发CC防护策略
应用防护	• 黑IP监控 • 黑IP阻断
业务防刷	• 白IP放过 • 灰IP下发验证码 • 黑IP下发验证码策略

* 可在腾讯云体验：宙斯盾&大禹



* 可在腾讯云体验：天御



未来

多学习，多摸索

广告时间

TSRC官网：http://security.tencent.com

“腾讯安全应急响应中心”微信公众号 ☞

新浪微博：@腾讯安全应急响应中心

官方邮箱：security@tencent.com

感谢您的关注！

Thank you for your attention