已经发生的未来

——从起因到完整形态，整体是各部分之和

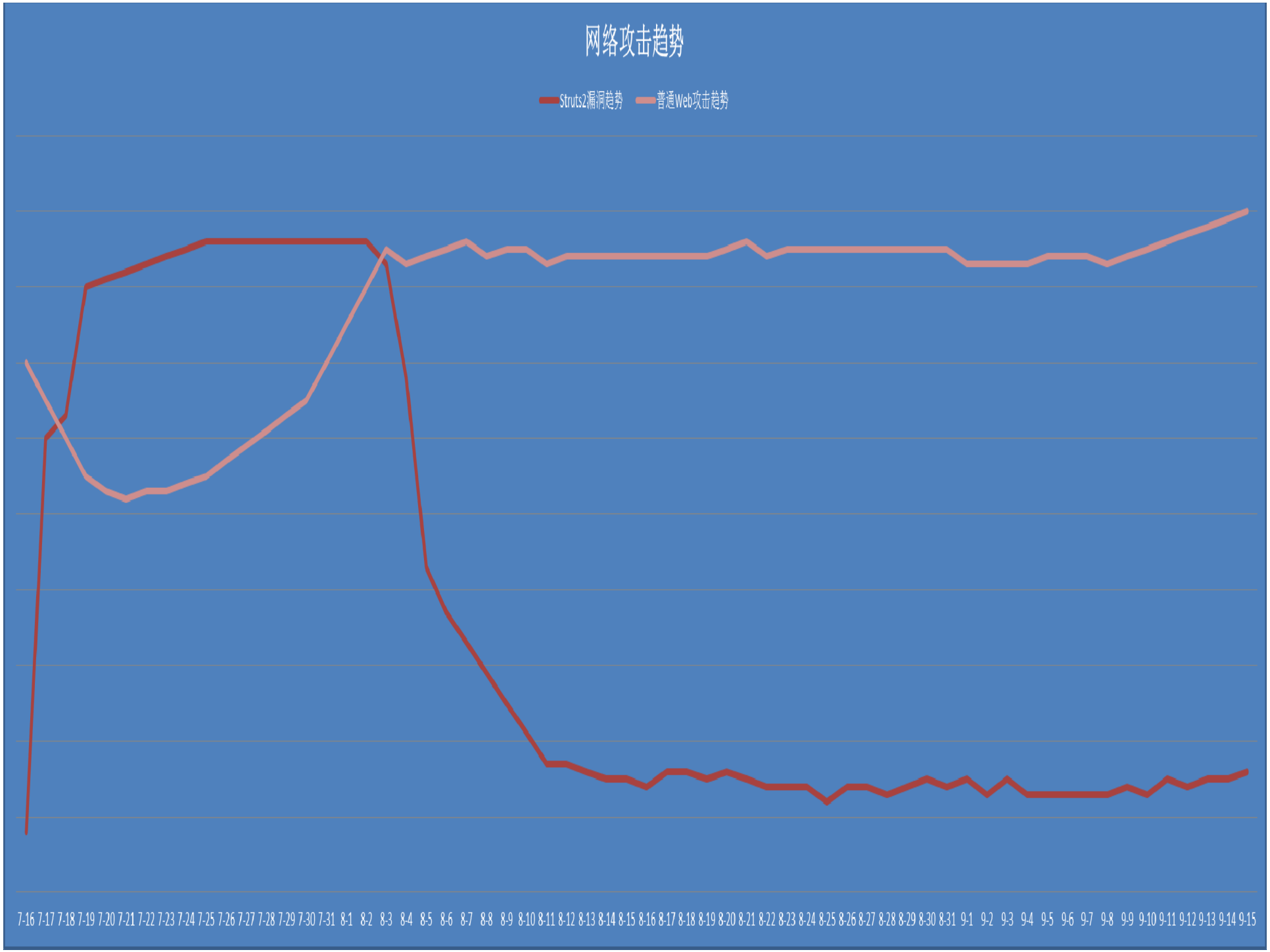
OWASP 中国

The Open Web Application Security Project

About me

- 林峰
- 知道创宇
- M：linf@knownsec.com
- @知道创宇应急响应中心 @KS临风

睡不好觉的事情有哪些？


网络攻击趋势
Struts2漏洞趋势
普通Web攻击趋势
7-16 7-17 7-18 7-19 7-20 7-21 7-22 7-23 7-24 7-25 7-26 7-27 7-28 7-29 7-30 7-31 8-1 8-2 8-3 8-4 8-5 8-6 8-7 8-8 8-9 8-10 8-11 8-12 8-13 8-14 8-15 8-16 8-17 8-18 8-19 8-20 8-21 8-22 8-23 8-24 8-25 8-26 8-27 8-28 8-29 8-30 8-31 9-1 9-2 9-3 9-4 9-5 9-6 9-7 9-8 9-9 9-10 9-11 9-12 9-13 9-14 9-15

0day被曝光之后

消息灵通的黑客

手工尝试

出现两款利用工具

利用工具优化更新

批量利用工具出现

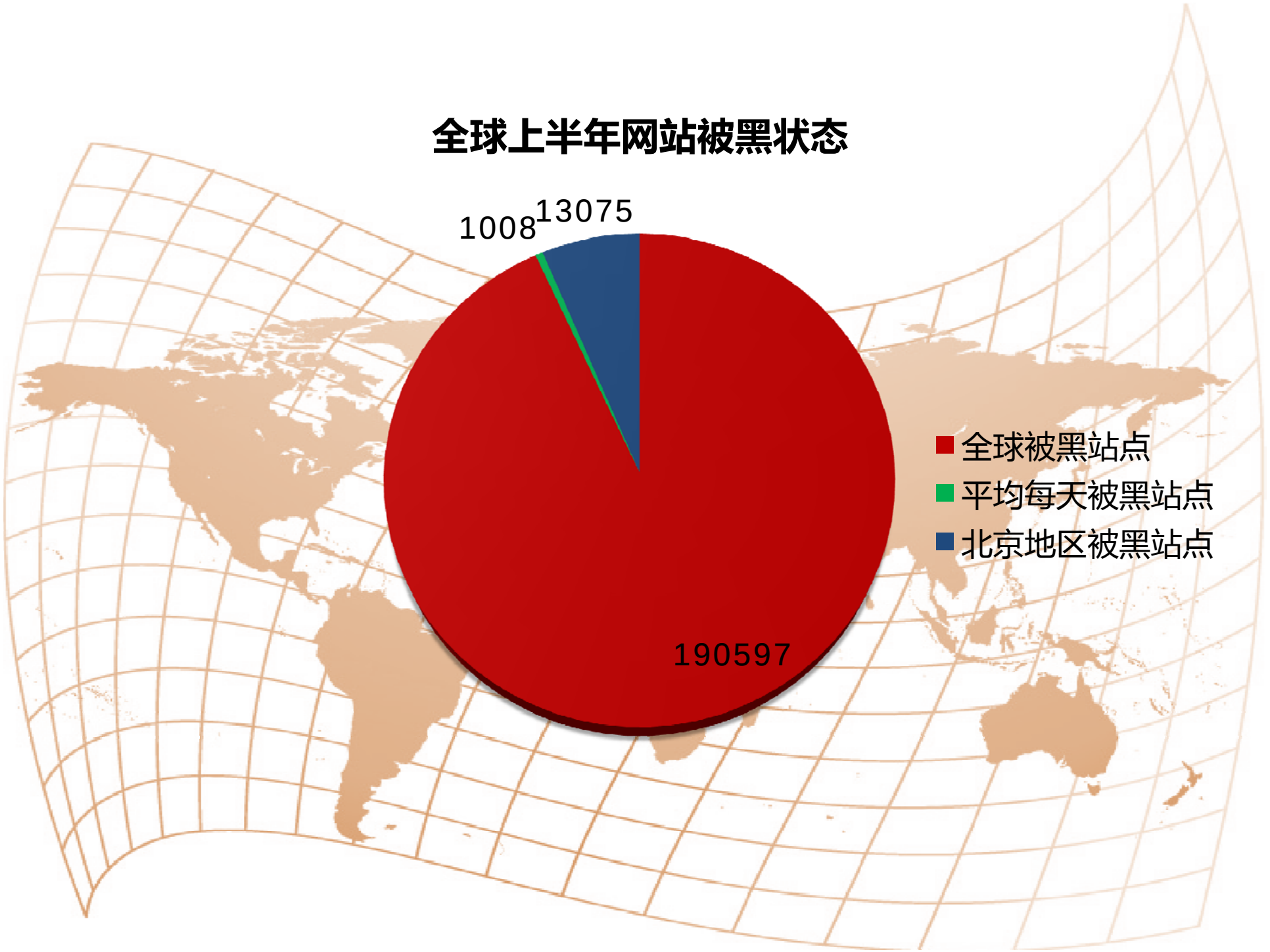
利用工具优化更新

工具更新伪装

工具利用型黑客

7天时间，10种攻击工具出现


安全产品漏洞
网络设备漏洞
操作系统漏洞
数据库漏洞
WEB应用漏洞
应用程序漏洞
操作系统漏洞
应用程序漏洞
WEB应用漏洞
数据库漏洞
网络设备漏洞
安全产品漏洞

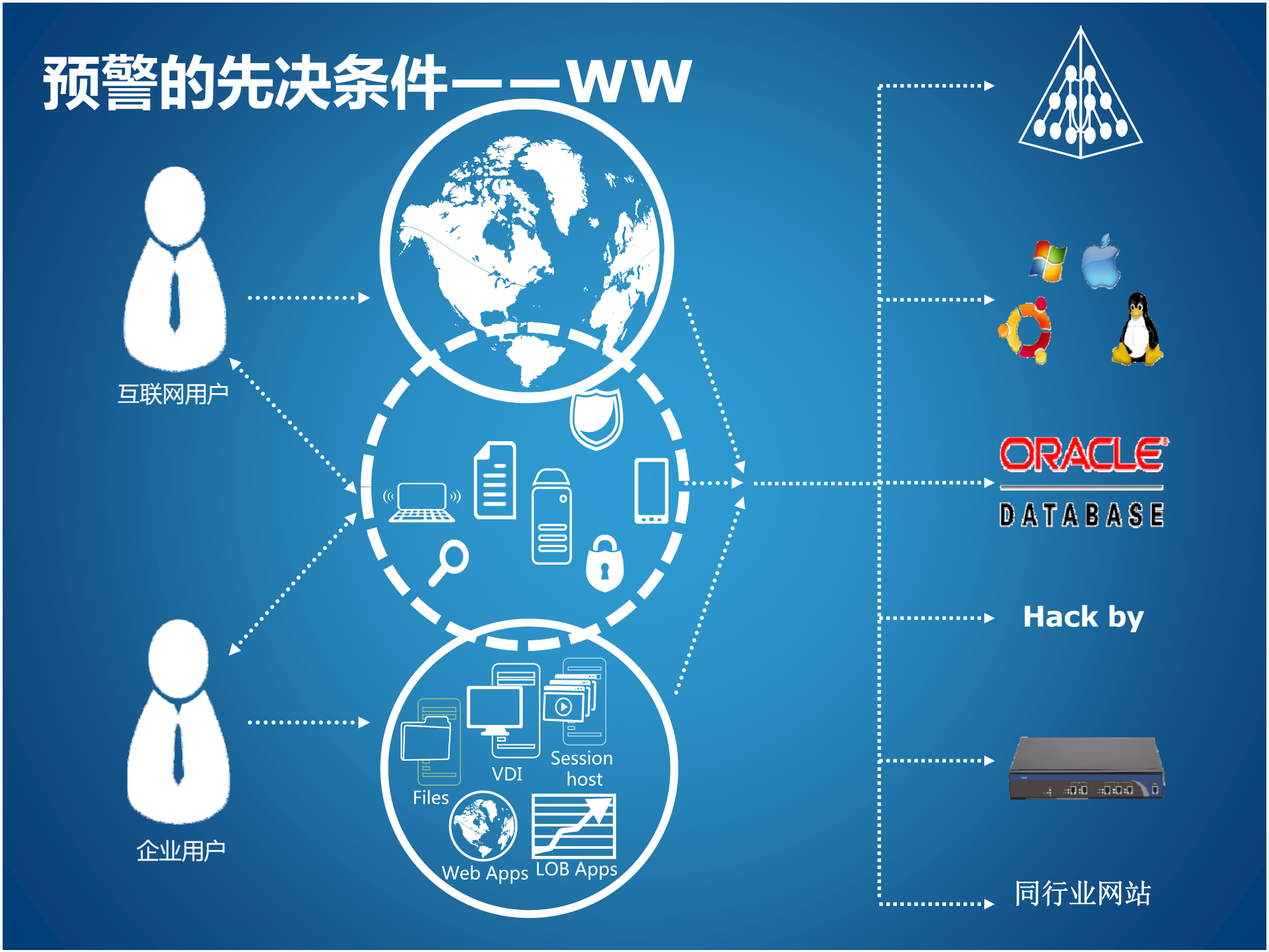

全球上半年网站被黑状态
1008
13075
190597
全球被黑站点
平均每天被黑站点
北京地区被黑站点

网络战争中什么最贵？

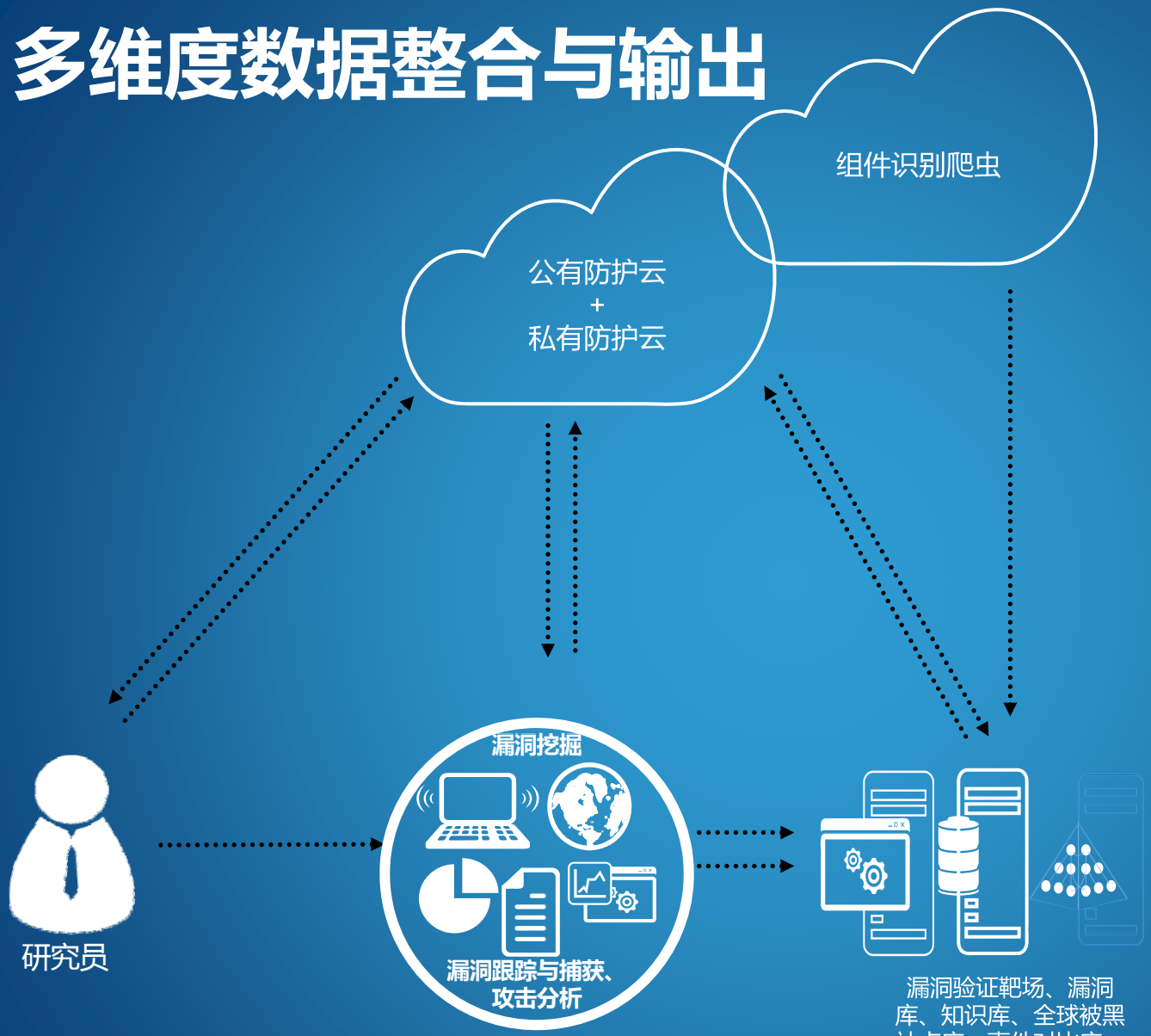
反恐！

基于大数据的预警实现

预警的先决条件——WW


互联网用户
企业用户
Files
VDI
Session host
Web Apps
LOB Apps
ORACLE
DATABASE
Hack by
同行业网站

多维度数据整合与输出



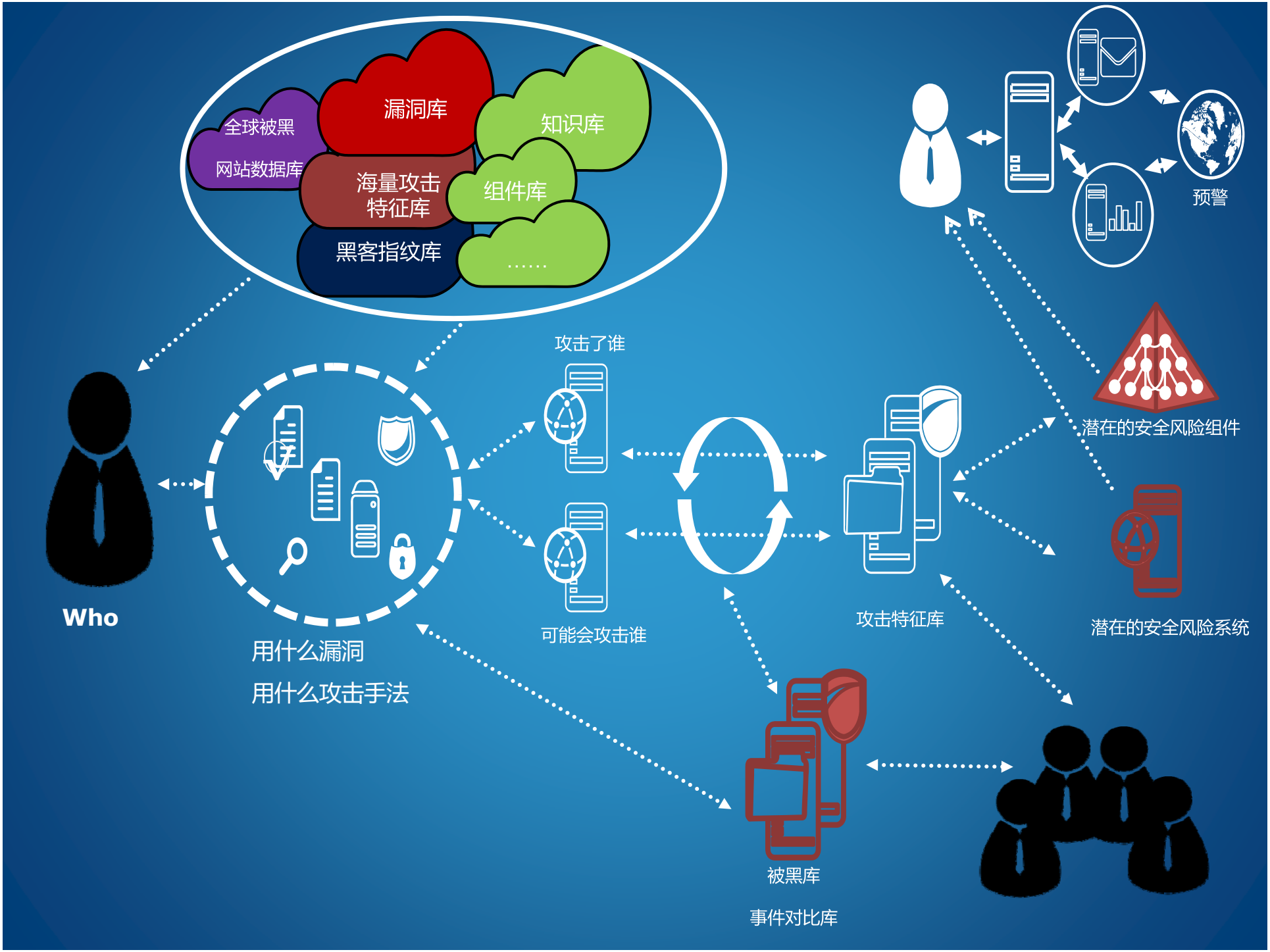
1. 安全研究人员挖掘、跟踪漏洞，分析攻击数据，组件识别爬虫，输出组件库

2. 漏洞防御规则等安全数据与云端同步

3. 云端捕获的攻击数据自动分析并输出到数据中心

4. 安全研究员分析攻击，与捕获漏洞，并输出研究成果

5. 数据中心分类输出需求库


全球被黑
网站数据库
漏洞库
知识库
海量攻击
特征库
组件库
黑客指纹库
……
预警
攻击了谁
潜在的安全风险组件
Who
用什么漏洞
用什么攻击手法
可能会攻击谁
攻击特征库
潜在的安全风险系统
被黑库
事件对比库

谢 谢