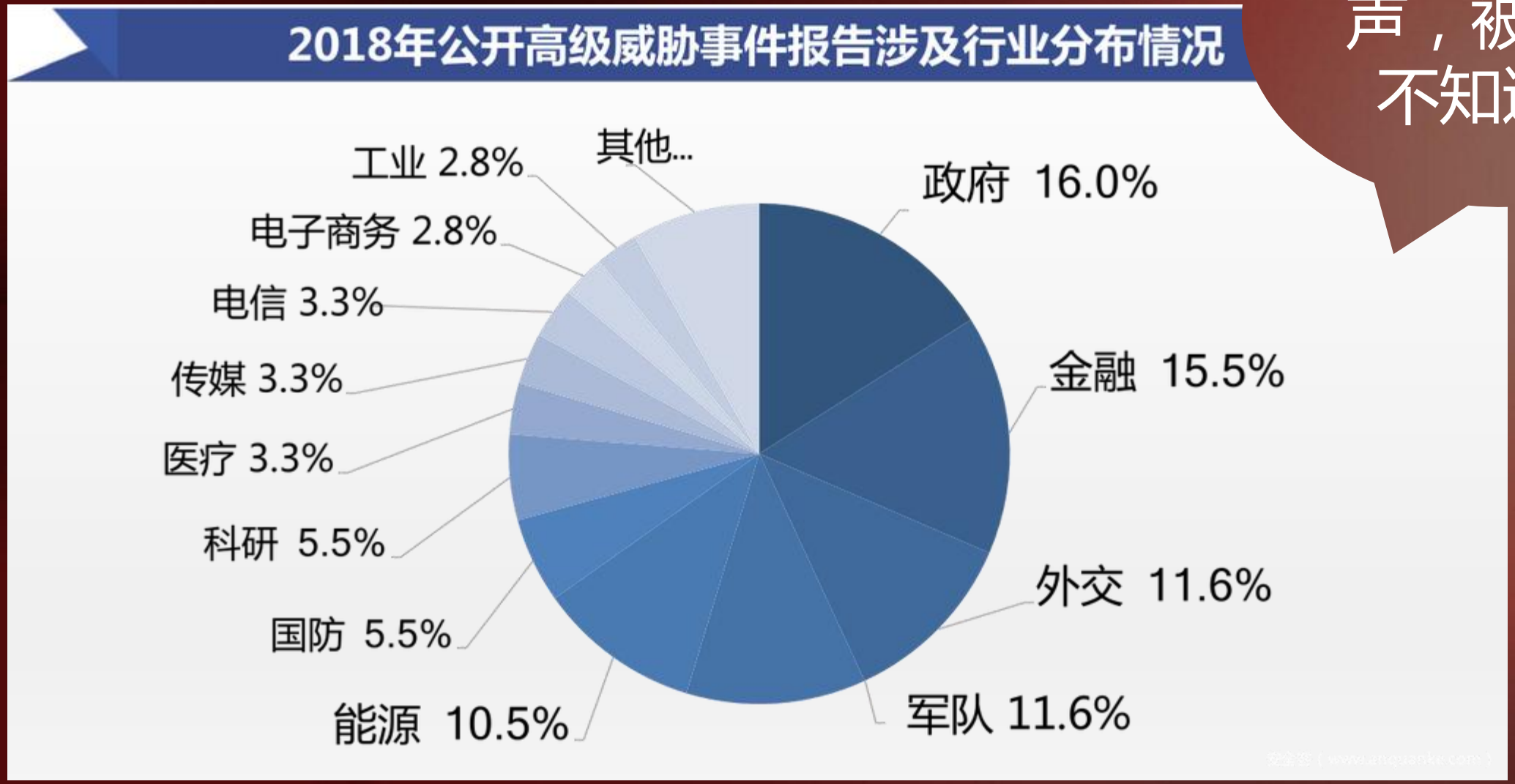
企业安全建设之红蓝对抗

OPC 2019/03/23

前言

被黑了不吭声，被黑了不知道？



安全建设的“马斯洛需求”层次

某某统计的产品
安全分类大全

- 裸奔状态
- 自认为是安全的
- 救火能力
- 安全体系化
- 业务层面安全得到保障
- 用先进的方式实践安全

网络安全	防火墙、入侵检测与防御、防病毒网关、上网行为管理、网络安全审计、VPN、抗拒绝服务攻击、网络准入等
端点安全	防病毒、主机检测与审计、安全操作系统、主机/服务器加固、HIDS等
应用安全	WAF、WEB安全扫描器、网页防篡改、邮件安全等 安全评估、渗透测试、代码审计、SDL、RASP等
数据安全	数据库审计与防护、安全数据库、数据泄露防护、文件管理与加密、数据备份与恢复
业务安全	账号安全、交易风控、征信、反价格爬虫、反作弊、反bot程序、反欺诈、反钓鱼、反垃圾信息、舆情监控、反游戏外挂、打击黑色产业链、安全情报等
身份与访问管理	运维审计堡垒机、数字证书、身份认证与权限管理、硬件认证等
安全管理	安全管理平台、日志分析与审计、脆弱性评估与管理、安全基线与配置管理、威胁分析与管理、终端安全管理、信息安全管理体系建设等

目录内容

- 红蓝对抗是什么
- 红蓝对抗的价值和意义
- 红蓝对抗的注意事项
- 红蓝对抗的点与面
- 红蓝对抗典型案例

红蓝对抗
“没有硝烟的网络战”

红蓝对抗的价值和意义

- 未知攻、焉知防
- 是骡子是马拉出来遛一遛
- 梳理风险盲点
- 提升安全人员的安全技能和防护水平

红蓝对抗注意事项

- ✓ 蓝队为企业内部人员或外部可信白帽子：
- 蓝队一般需要将攻击目标、攻击方式、何种漏洞、渗透思路、可能造成的攻击后果或故障等向紫队报备；
- 蓝队在测试过程中需保持通讯畅通，在演练过程发生灾难时可以及时联系到并暂停或停止测试；
- 蓝队一般不被允许发起任何形式的DOS或DDOS攻击
- 蓝队被禁止对目标系统和业务造成破坏和干扰
- 蓝队被禁止对系统重要数据进行获取、篡改等
- 蓝队获取数据条数及文件总量受到限制
- ✓ “蓝队”为真正的攻击者：
- 红队需要注意，上述注意事项“蓝队”很大可能不会遵守

红蓝对抗中的点与面

- 初始通路（10项）：硬件添加、鱼叉式钓鱼附件、供应链妥协、正确的账户密码...
- 命令执行（33项）：命令行界面、计划任务、 MSHTA 、PowerShell...
- 后门稳固（58项）：.bash_profile和.bashrc、浏览器扩展、正确的账户密码、 DLL搜索顺序劫持...
- 权限提升（28项）：辅助功能、EXP 0day、有效账户、webshell、路径拦截、 DLL搜索顺序劫持...

红蓝对抗中的点与面

- 绕过防御（63项）：代码签名、 NTFS文件属性、禁用安全工具、二进制填充...
- 凭证获取（19项）：抓明文密码、文件中的密码、密码过滤DLL、 .bash_history ...
- 信息搜集（20项）：账户信息、文件和目录信息搜集、浏览器书签信息搜集、网络共享信息搜集、安全软件信息搜集...
- 横向移动（17项）：哈希传递、Pass the Ticket、远程文件复制、远程桌面服务...

红蓝对抗中的点与面

- **数据拷贝（13项）：音频捕获、电子邮件、来自本地系统的数据、网络共享驱动器中的数据、屏幕截图...**
- **数据外传（9项）：数据压缩、数据加密、数据传输大小限制、预定转移...**
- **命令控制（21项）：常用端口、数据编码、数据混淆、远程文件复制...**

红蓝对抗典型案例

- 案例1
- 案例2
- 案例3
- 案例4

REFERENCE && Q&A

ATT&CK Matrix for Enterprise
https://attack.mitre.org/

Thanks !