真实环境下的红蓝对抗与协同

张嵩

数据泄露距离我们多远？

根据“补天平台”的数据，因为软件漏洞的存在… …

金融行业 态势严峻 | 平均每天可泄露110万条金融数据

2016年，高危漏洞

1992个，涉及159家机构

39979.4593万条

可轻易、直接泄露

关于“攻陷” ，FireEye怎么说？

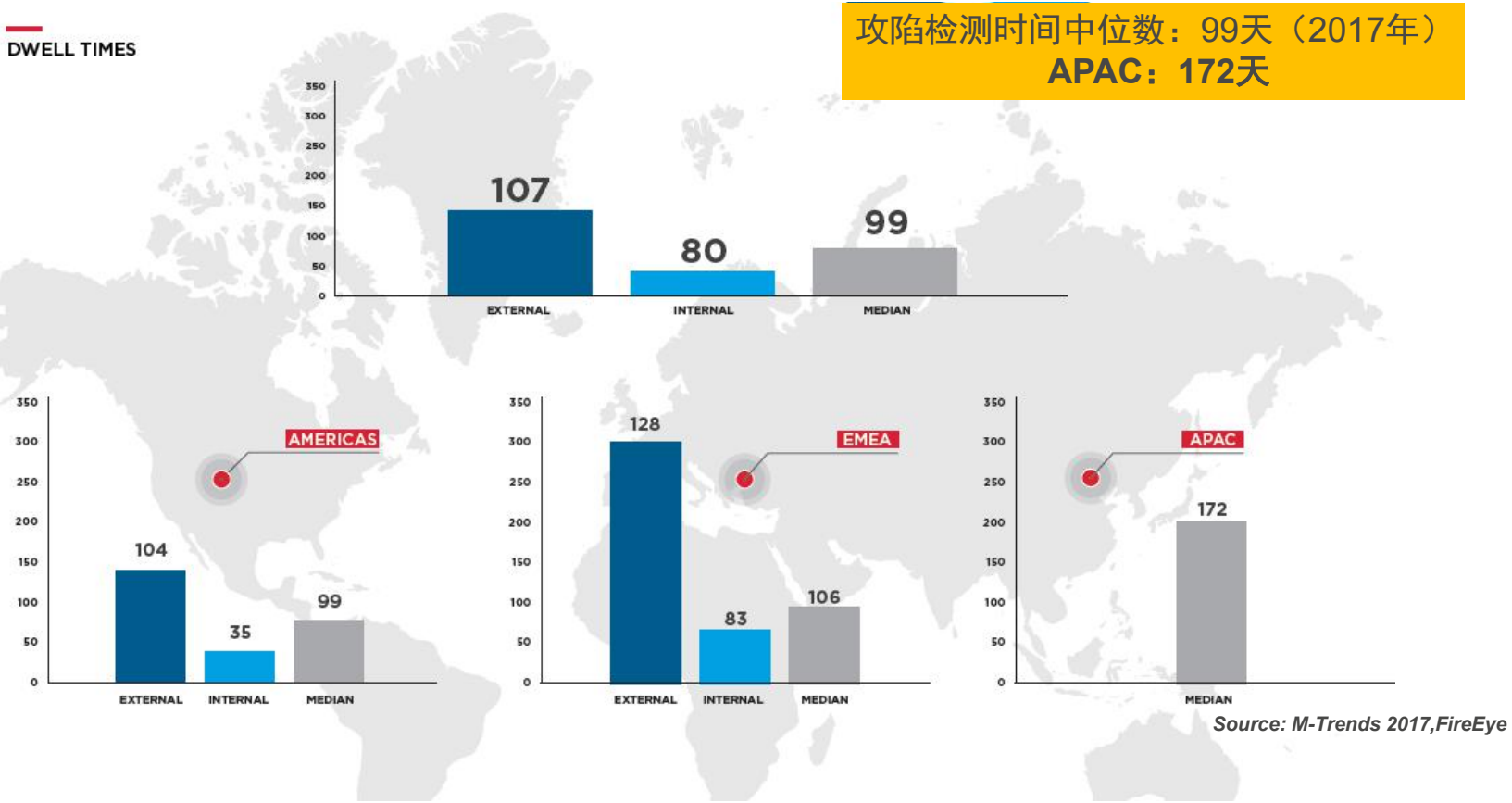
The Ultimate Detection Metric:
Reductions in Dwell Time

攻陷检测时间中位数：146天（2016年）

Source: *M-Trends 2016, FireEye*

关于“攻陷” ，FireEye怎么说？

攻陷检测时间中位数：99天（2017年）
APAC：172天



Source: M-Trends 2017,FireEye

Verizon 数据泄露调查报告2015—国际金融服务机构

FIGURE 2
TIME TO DISCOVER AN INCIDENT IN FINANCE

38%的国际金融机构需要数“月”的时间“感知”一个可导致泄露的事件；
21%的机构需要几周到几个月的时间“应对” 事件和外部威胁

国际金融机构攻陷检测时间在降低，中国呢？

Verizon 数据泄露调查报告2016—国际金融服务机构

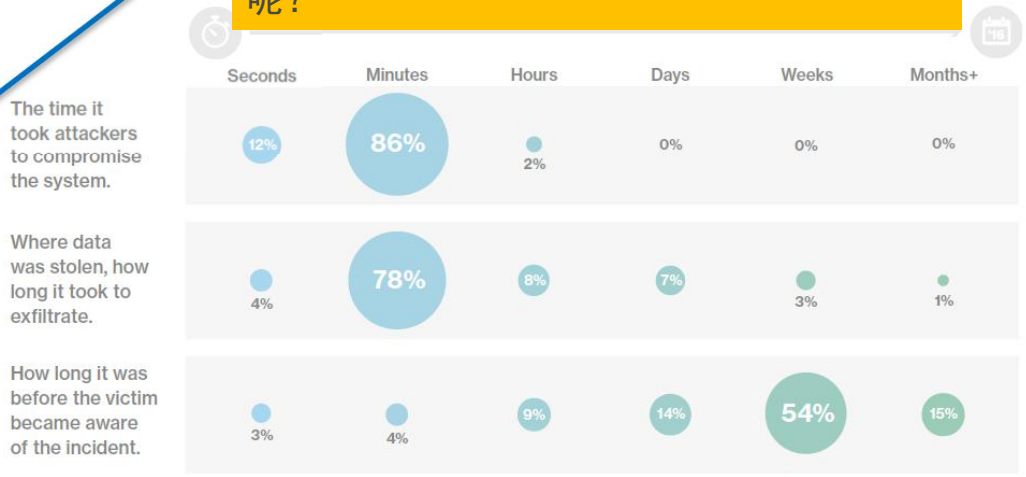


Figure 2: Incident timeline for financial services

54%的国际金融机构需要数“周”的时间“感知”一个可导致泄露的事件；
23%的机构可以在“几个小时到几天”的时间内“感知”

拿下一片数据中心区域，
难吗？
Let’s see~

一个真实威胁应对过程：Struts2-045 重大漏洞案例分析

应急“生命线”

开始产生实质安全影响

监管影响开始产生

1Day漏洞

在此时间前，漏洞仅在小范围内流传，尚未形成大范围攻击，受影响范围有限。

15点左右，攻击工具开始广泛在互联网流传

18点，白帽子提交了关于“某公司”的漏洞；经证实，是“同名公司”的漏洞

截止18：00，包括多家金融机构漏洞被利用获取权限的截屏已经可以在互联网获取

两会期间，一个漏洞平台的统计口径，据不完全统计，白帽子发现了69家金融机构的重大漏洞，引起监管层高度关注：涉及国有四大行1家，股份制银行2家，城商行20家，保险行业机构21家，证券基金机构9家，互联网金融机构16家。

部分金融机构因此漏洞收到监管部门通告

19：00 Apache发布漏洞公告、修复更新

23：00 安全运营人员获得漏洞情报，判断影响级别为极其严重

某金融监管机构下文，要求行业机构高度重视；监管部门请第三方机构对金融机构进行测试

两天，一个漏洞平台收到白帽子提交的全国漏洞10000+；被黑客、境外势力利用的数据无法统计

第1日 | 2 | 3

0Day漏洞

在公开发布之前的漏洞。仅仅被国家、极少数黑客或者技术研究人员知晓和利用。

9：00 安全响应人员启动应急，通知受影响资产的管理员，统筹修复策略；系统管理人员开始行动

10：00 安全响应人员联系情报社区、外部合作机构获取漏洞利用工具（POC）。初期，POC只在非常小的范围流传

12点，安全响应人员从小范围安全社区获取高质量的漏洞利用工具，并开始对内部系统进行测试

13点-18点，陆续完成修复

- 13：00，第一个系统升级修复完成
- 14：58，第二个系统升级修复完成
- 18：10，第三个系统升级修复完成

19：10 三个系统的修复验证完成

18：00，厂商I通过自定义策略，暂时防护

8：00，厂商P发布防护策略更新

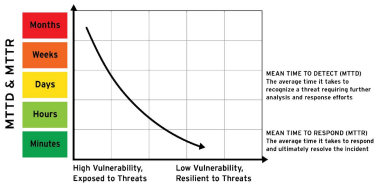
第二日晚至第三日，国内厂商陆续公布各家设备防护策略

第4日，厂商C发布防护策略更新

退回生命线内

全体IT人协作目标

MTTR 持续降低



MTTR—应急响应时间

注：修复、验证时间为演示目的虚构时间；生命线左侧时间为一般安全资源企业估计的时间

如何利用Struts2漏洞拿下一片数据中心—技术篇

一下手头的清单，确定存在Struts2漏洞；确认中间件运行权限(通常为root或system，最高权限)

无需Deliver阶段

1-2分钟，确定web应用物理路径并上传webshell

Mimikatz抓取当前服务器会话的明文密码，没有会话的用户抓取哈希后通过哈希获取密码

5分钟，扫描当前C段存活主机

在官方出公告后的**24小时内，**POC、攻击代码快速流传

1分钟，远程执行Struts2攻击脚本，利用漏洞

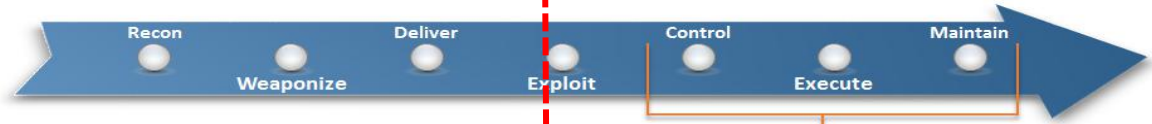
10分钟，初步收集敏感信息(网络连接情况、数据库连接字符串、web应用管理员密码等)

5分钟，分析归纳管理员用户名、密码与主机名、应用类型、IP等信息的关联，根据规律生成密码

5-10分钟，使用生成的密码字典对存活的主机进行爆破并成功横向渗透到相关主机

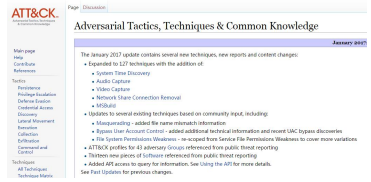
Proactive Detection
Mitigation

Incident Response & Mission Assurance

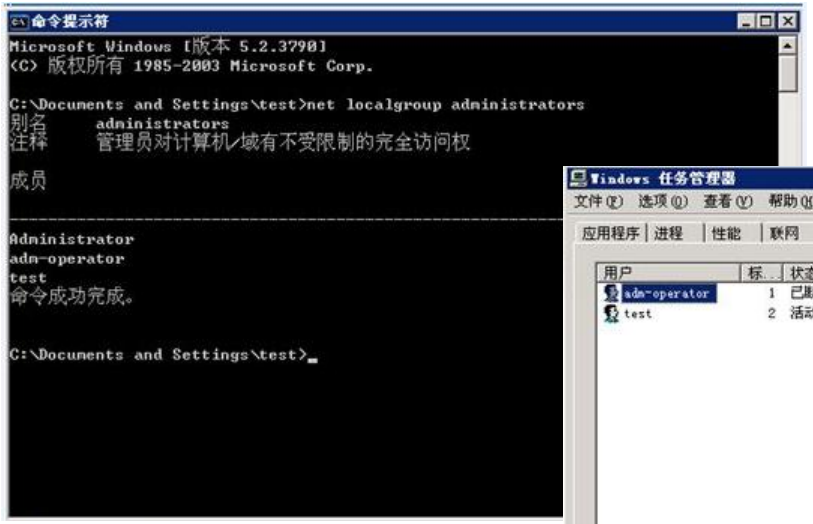


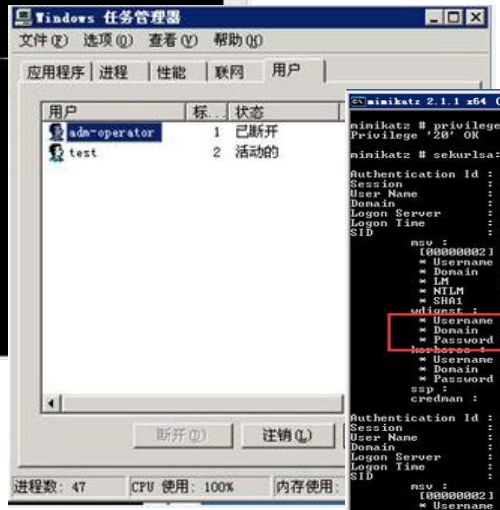
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Execution
Collection
Exfiltration
Command and Control

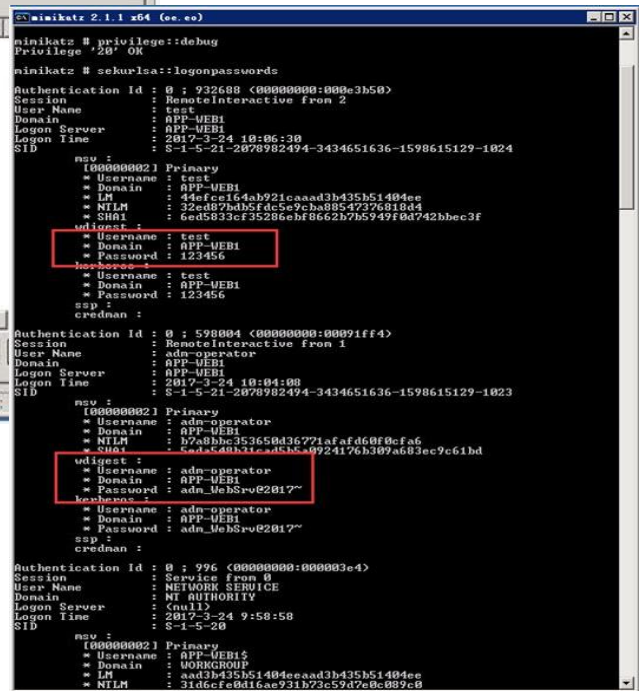
MITRE



读取口令







- 通过Struts2 漏洞添加名为test的管理员 用户
- 登录系统后查看管理员组成员
- 确认当前系统会话情况：
  - test在线，adm-operator用户断开
- 用Mimikatz读取当前所有会话用户的明文密码
- 用Mimikatz读取Administrator的Hash

企业何去何从？

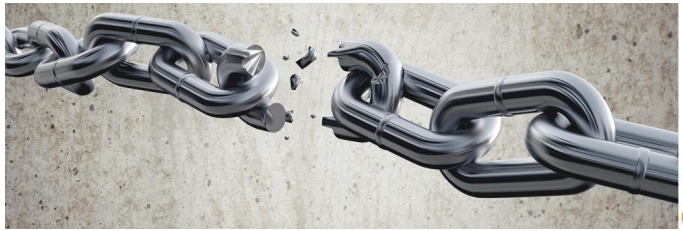
企业安全理念的转变：从~“不出事”，到~打破攻杀链，随着威胁管理的成熟度提高，检测、响应时间降低

“雅虎们”的现身说法：

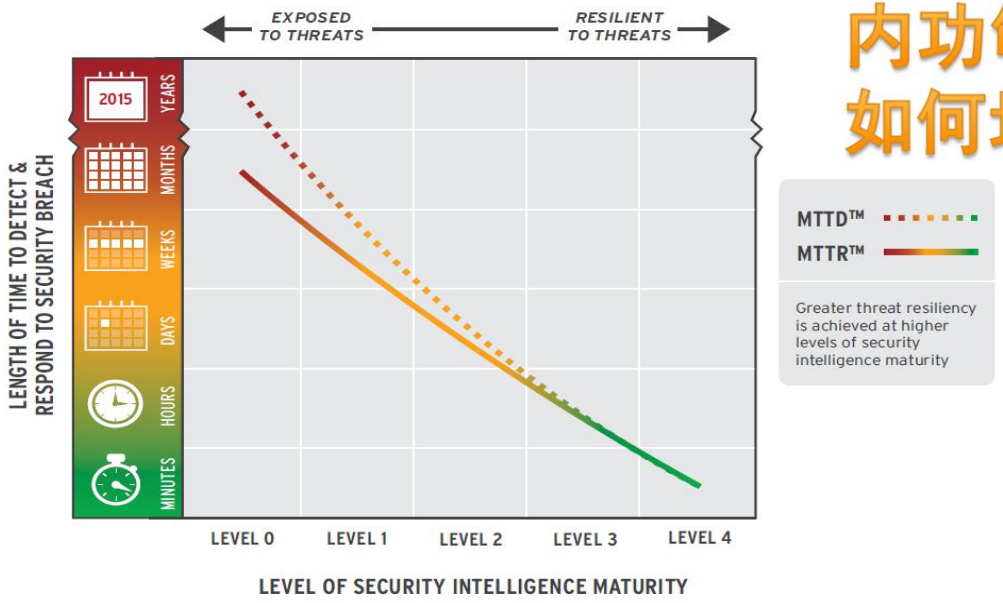
不出事儿恐怕是不可能的！

多久可以发现？

应对？



真实环境对抗，内功够吗？如何增强？



企业安全需要多支队伍：红、蓝、紫

企业安全需要多支队伍：红、蓝、紫

老板，
缺人缺技能！
需要外部辅助
检测与应对！

企业，
你又搓了！

Red Teaming—企业内部安全人员：

- 大量在“运维”
- “防”：网络与主机安全防护
- “攻”：软件安全测试、渗透测试
- “响应”：威胁发现、应对，威胁猎捕

Blue Teaming—企业外部安全人员：

- 白帽子

- 传统企业内部蓝军
- 传统外部渗透测试人员

抱歉，
安全公司也缺人！

Purple Teaming—企业外部技术顾问人员：

- 众测过程中的观测、指导
- 众测结果驱动的安全架构、运营和技术措施咨询与优化
- 咨询如何检测、应对“Mimikatz”们，感知真实攻击
- 讲解黑客、黑产套路，如何躲避防御和检测
- “导演”红蓝对抗演习；以“教育”为目的高级测试、演练
- 应急响应、调查取证、Threat Hunting、MDR、MSS
- 辅助企业建设可运营的SIC、SOC，优化安全分析过程、效率

企业，莫慌
我来教：
为什么搓了？
如何在同一个地方
不再搓！

Takeaways–Purple Teaming的结

- 对白帽子还在纠结？ 平衡下有和没有白帽子哪个风险大
- 安全服务人员和白帽子需要协同，各有专攻
- 传统堆设备的安全方法，带来的只是一种虚假的安全感
- 红蓝对抗演习验证了“假设攻陷”理念；思想转变以后，感知到的是不同的景象
- 没有不透风的“墙”