



★ 本期焦点

关于下一代安全的几点思考

网络钓鱼产业链分析

攻击者想要什么

浅谈下一代防火墙的现状 & 未来

### 本期看点 HEADLINES

2 关于下一代安全的几点思考

8 网络钓鱼产业链分析

14 攻击者想要什么

29 浅谈下一代防火墙的现状和未来



主办：绿盟科技  
策划：绿盟内刊编委会  
地址：北京市海淀区北洼路4号益泰大厦三层  
邮编：100089  
电话：(010)6843 8880-8669  
传真：(010)6872 8708  
网址：www.nsfocus.com

# 2011/09 总第 014

Nsmagazine@nsfocus.com

## 安全+ SECURITY+

© 2011 绿盟科技

本刊图片与文字未经相关版权所有人书面批准，一概不得以任何形式、方法转载或使用。本刊保留所有版权。

SECURITY+ 是绿盟科技的注册商标。

需要获取更多信息，请访问WWW.NSFOCUS.COM

<b>专家视角</b>	<b>2-31</b>
关于下一代安全的几点思考	赵粮 2
网络钓鱼产业链分析	谭荆利 8
攻击者想要什么	颜涛 14
企业移动设备安全管理方法与实践	王卫东 24
浅谈下一代防火墙的现状 & 未来	段继平 29
<b>行业热点</b>	<b>32-58</b>
浅谈蜜网在电信运营商行业中的应用	唐洪玉 32
金融机构反钓鱼监控体系建设方案	陈星霖 37
美国《网络空间国际战略》解读	李文法 孙铁 43
银行各类部门在 IT 风险管理体系中的职责	徐一丁 50
软件自动化测试实践	李志昕 54
<b>前沿技术</b>	<b>59-71</b>
Adobe Reader X 保护模式技术分析	赵亮 59
图像识别在钓鱼检测中的应用	张鸿勋 67
<b>绿盟动态</b>	<b>72-73</b>
<b>安全公告</b>	<b>74-76</b>
NSFOCUS 2011 年 7 月之十大安全漏洞	74

# 关于下一代安全的几点思考

安全研究院 赵粮

**摘要：**本文总结了对安全业界当前实践的三个观察，提出了下一代安全体系的可能发生的三个变革—更加智能、面向服务及行业精细分工。应该看到，这些思考还是粗糙的、不成系统的，在逻辑上也不完整，仅供大家讨论参考。

**关键词：**云计算 虚拟化 面向服务架构 SOA 人工智能 下一代安全架构 下一代网络安全

## 1、前言

坦白说，写本文的主要目的是反思，反思的目的是探讨和研究潜在可行的变革和创新。

虽然网络安全作为一个产业已经走过了十几年的历程，但是应该看到网络安全产业界还处于一个相当不成熟的初步阶段，作为行业里的一个老兵，这样说内心里很不舒服也不情愿。对于行业实践中的这些“不成熟”，笔者在技术内刊总第 8 期“网络安全发展的战略回顾” [ZL1][ZL2] 中已有不少列举（以下简称战略回顾）。举例说：

- 网络安全相当程度上依赖于基于 IP 五元组之上的边界防护模型，明显落后于互联网和 IT 应用技术的发展；
- 产业界尚未形成相对成规模的产业内分工，大多数用户和提供

者处于低于规模水平的运作状态；

- 产业界的大部分维护建设工作由人工完成，自动化程度很低；
- 网络安全设备种类繁多，之间缺少有效的集成和互动，智能化水平很低；
- 保护对象的业界缺少相对完备和公认的方法工具等评价安全投入的产出价值。

所谓“下一代”是一个很模糊的词，本身并没有确切的时间段来区分，有点和稀泥的意味。在“战略回顾”一文中，描述了过去十多年时间里 0.1、1.0、2.0 三个时代各自的特征，也尝试着提出了 Security NG 的一些猜想。本文的“下一代”在“战略回顾”一文基础上，尝试将“下一代”更加具体化，与业界的实践建立更多的联系。

本文后面三节分别拣选了三个方面，探讨当前安全实践中可能存在的“问题”。第2节将分析当前安全实践中基于IP五元组的“城堡”防护模型，第3节将分析以硬件盒子为主的安全产品形态方面的问题，第4节将分析安全产业在分工和互信、互动方面的问题。同时，在每个小节也提出了相应的下一代安全体系的可能特征。

## 2、从城堡向智能化安全演化

考察其工作机理，当前以防火墙（或者



图1 古代城墙与现代都市

UTM)、入侵检测、漏洞扫描为主体的网络安全体系，相当程度上，主要依赖于基于IP五元组之上的边界防护模型。

打个比方，当前的网络安全体系有点像古代的城堡，将重要资产（例如数据中心、企业网等）使用高高的城墙团团围住，设立几个坚固的城门和吊桥来检查放行被认为“安全”的人、货物、车辆等。

在古代，因为经济活动简单、城市规模很小，城墙+城门的架构很好地满足了安全和交通的“平衡”需求。随着城市规模的扩大和攻防武器的进步，城墙成为都市奢侈的观光景点。现代城市的安全系统演变为分布式的视频监控系统、移动巡查系统、快速响应系统等，城市的安全性和方便性（性能）获得新的平衡。

我们看到，近两年来，基于应用、用户和内容的安全控制已经随着下一代防火墙概念的逐渐普及获得了越来越高的重视。其背后的原理是因为数据和用户（What, Who）在云计算和移动互联网年代要比基于IP的位置（Where）更为稳定，相应制定的安全策略更贴近于业务的实际需求。

基于应用、用户和内容的安全控制比“IP五元组”先进了很多，但是还远远不够。

## 智能化

智能化（intelligent）的安全是相对于当前机械的、基于既定IP五元组和已知手法的安全来说的。

人工智能是智能机器所执行的通常与人类智能有关的功能，如推理、规划、解决问题、抽象思维、理解复杂概念、从经验学习等 [AI]。人工智能从正式被提出作为一个学科已经有40多年了，从学术、技术到应用都取得了长足的发展，直接促成了很多生产领域的“革命”。举例说，目前电信运营商和互联网公司都普遍地采用人工智能（数据挖掘）技术提高客户分析、收入保障、决策支持、业务推荐等相关能力和客户体验。

网络安全领域，目前普遍来看，人工智能技术的应用领域还非常匮乏，限于一些基本的基于规则或策略的相关处理。这个发展不足有各方面的原因，但是缺少足够数量的、质量较高的数据，被认为是目前网络安全领域走向更进一步“智能化”的一个关键

瓶颈。

例如，安全业界普遍匮乏实际的运营指标、运营记录、安全事件、事件根源分析等基础数据，所谓“最佳实践”大多是建立在各种调查问卷以及安全顾问和专家的个人经验及观察上的。这些调查问卷大都没有公开调查问卷的问题设计、答卷人的分布和选择过程、分析过程等，经常看到各种调查问卷结果之间的相互矛盾和冲突，结果并不十分可信 [NewSchool]。

同时，大量的各种各样的安全设备每天都产生海量的各种数据（例如日志和告警），但是，业界缺少安全数据相关的标准，并且对

安全“元数据”的重视也远远不够，这些原因都间接地弱化了安全“智能化”的基石，同时也大大限制了安全管理中心（SOC）类产品（或称为解决方案）的实际功能效果，只能徘徊于在较为狭窄的“事件管理”领域，无法提供更高价值的策略优化和决策支持等功能。

有专家提出业界需要进行一系列关键变革来“修复”当前 SOC 实践的这些不足 [SOC]，如图 2 所示，其中“智能化”是一个关键。

除了在 SOC 的“智能化”之外，安全信誉技术 [LXP]、安全态势感知 [WWD][LWF]、行为异常检测等概念、理论和模型被提出来并逐步得到应用。这些“智能化”努力都是下一代安全体系建设中的重要环节。



图 2 SOC 需要进行一系列关键的变革

### 3、从硬件向服务演化

在前面的十多年实践中，硬件盒子在安全产品中大兴其道，占领了大部分的市场份额。硬件盒子本身并无对错，只是当我们把目光转向所保护的业务和应用时，却发现它们已经发生了很大的变化。

从早年的中间件、企业应用集成 EAI、面向服务架构 SOA，到近年的虚拟化和云计算，数据中心本身和应用计算架构的“焦点”已经逐渐由“硬”变“软”，变得越来越“虚拟”。以看似琳琅满目、大大小小的硬件盒子，构成的网络安全解决方案在满足用户需求、适应用户环境上越来越吃力，如图 3 所示。这一点在互联网企业的安全需求和解决方案上显得最为突出。

“吃力”不仅仅是因为技术架构和集成方面的距离，并且在硬件、软件、服务、虚拟镜像等的运维、要求的技能、相关配置变更等流程、财务等方面，都不尽相同。

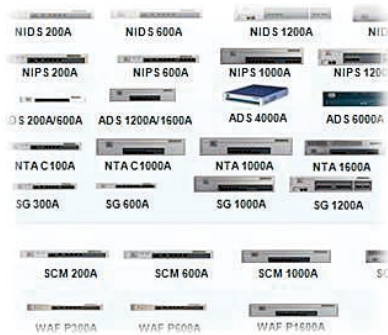
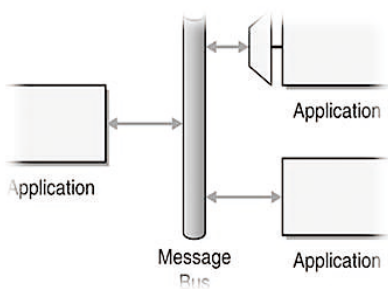


图3 硬件盒子的产品形态难以适应“虚拟”化的计算环境

## 面向服务

面向服务架构 SOA 的提出已经有很多年了 [SOA], IT 服务管理 (ITSM) 也提出有很多年了, 两个“服务”都已经获得广泛的认可和部署, IBM 还提出了服务科学的概

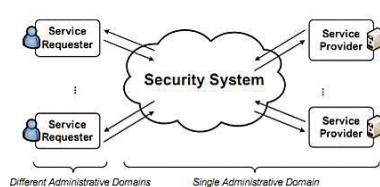


图4 安全“服务”的提供者和消费者

念 [IBM]。面向服务的、松耦合的架构, 成为解决复杂系统设计的一个重要方法, 而 IT 运行维护服务化, 则成为现代 IT 业正在逐步走向成熟的标志之一。

“服务”有很多意味, 服务意味着提供者和消费者, 服务意味着可以度量和计价, 服务意味着松耦合、开放和分工……如图 4 所示, 安全“服务化”将提供者和消费者显式地分离开来, 他们不必是同一个管理部门、不必是同一个开发厂商、不必是同一开发平台或语言……

账号认证授权或许是最早被“服务化”的安全产品。后来, 漏洞扫描和评估、日志服务、安全事件监视管理等也加入到安全“服务”清单上来。目前, 在云计算和软件作为服务 SaaS 的浪潮下, 云安全联盟已经设立了安全作为服务 (SECaaS - Security As A

Service) 的专门工作组, 并准备在云安全指南的第三版中, 为安全作为服务增加专门的一章。

面向服务的安全架构 (SOSA - Service Oriented Security Architecture) 是 SOA 和 SECaaS 的结合点 [SOSA], 从目前的研究和实践来看, 也存在很多挑战。例如安全元数据的设计和标准化、任务的调度、系统的复杂度和性能, 以及测试验证难度等。

应该注意, “服务”和“硬件盒子”并不是相互替代的关系, 而主要是“焦点”的转移, 就如同数据中心发生的云计算“演化”, 也有点像浏览器和操作系统之争。

## 4. 从 DIY 走向精细分工

行业里的同行们并不“快乐”, 或者说, 安全的用户和提供商有很多“痛”。“痛”有很多原因, 从用户方面来看, 可能由于:

- 缺乏专业人员、知识技能、各种资源;
- 认为安全供应商不了解用户的业务, 对提供商的服务及时性和效果都不满意;
- 安全产品很封闭, 用户无法自助配置来快速满足业务需求;

• 安全产品防护效果不佳，对大量涌现的各种网络攻击和恶意代码感觉无能为力，或者“慢半拍”，等等。

从安全供应商方面来看，“痛”可能由于：

- 对用户各种产品和服务定制要求觉得“无理”和“应接不暇”；
- 安全产品越来越难驾驭，到处都是“信息孤岛”，难以集成、关联
- “服务”价格很低，或经常被“搭送”；
- “用户产出”很不稳定，资源和能力都很难相应规划；
- 用户不愿分享，缺少机会了解用户的业务和安全产品实际运行情况，对突然的安全事件无法针对性的及时响应，等等。

以某些典型用户的运维活动为例，或许可以发现一些端倪。如图 5，大部分安全运维资源投入到了安全补丁、身份管理、安全事件响应、漏洞扫描和评估、安全配置检查稽核，以及其它各种由于缺少安全技能和工具导致的“救火”活动上；除此之外，有少部分的资源，可以投入到防火墙入侵检测等安全设备策略的检查和调优、安全总体状况评估、将安全嵌入建设项目和配置变更管理流程等；最少部分的资源，投入到了深入了解业务的内在安全需求、安全核心能力的开发与供应商管理等。

但是事实上，大部分网络安全的管理者和专家都认为，安全资源投入的产出价值与投入是相反的。也就是说，目前投入产出高的部分、最值得投入资源去做的事情，却因为金字塔底部的重复性操作的拖累而无法投入。

缺少有效的“分工”以及“规模”效应，是目前行业整体运营效率较为低下的一个主要原因，也是行业不够成熟的一个重要特征。

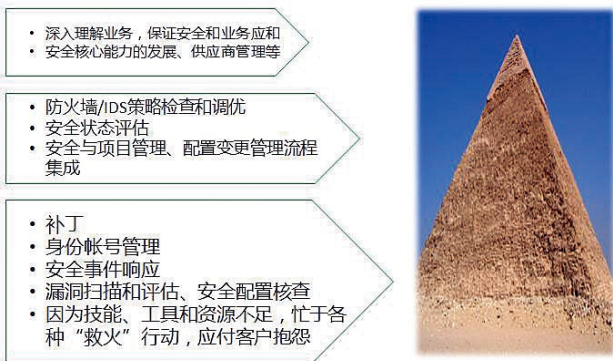


图 5 安全运维资源之金字塔分析

### 用户和提供商建立互信和精细分工

从亚当斯密出版国富论开始，到当前互联网和云计算奉行的“半成品时代”理念 [WBF]，每一次重大的产业革命都伴随着重要的行业间和行业内的重新分工。

云计算是催化剂，其本质是计算和 IT 作为服务提供，提供者和消费者分离，各自更加专注，实现规模效应，并且提供商方面得以通过云服务、云接口等新形式重新整合供应链，并保持很大弹性。

云计算作为一种思想，将会“催化”网络安全业内的决策管理层的思路，重新评估不同细分领域的投入产出，行业内的纵向分工将会出现更多的机会。

来自网络安全，尤其是数据安全方面的顾虑，一直是阻碍安全外包和数据分享的重要原因之一。随着相关法律法规的逐步完善，安全提供商在企业运营和内控方面也逐步走向成熟，用户和提供商、



提供商之间的互信关系将会逐步建立起来，走向精细分工的阻碍将会进一步弱化。

## 5、结束语

网络安全作为一个行业规模不大，但是涉及的技术和产品却很复杂，数十种“主要”的产品类别，复杂到即使是一个资深专家也不一定能说得全、说得清楚。行业里的产品提供商很多，规模又相对偏小。“复杂”碰到“偏小”或许是国内行业整体生产效率相对偏低的原因之一。

文中提了不少问题，不过从积极的角度去理解，这些问题也可以被看作“未被满足的需求”，用一句话总结就是，下一代安全体系将会具备智能化、面向服务、更加精细化的分工和互动等基本特征。

本文观点，不代表任何组织机构官方意见，限于笔者学识和所掌握信息，难免挂一漏万，请各位读者明察指正。

## 致谢

本文部分原始图片取自互联网，主要参考和引用已注明链接和出处，恕不一一致谢。

## 参考文献

[AI] [http://en.wikipedia.org/wiki/Artificial\\_intelligence](http://en.wikipedia.org/wiki/Artificial_intelligence)

[IBM] <http://www.slideshare.net/ifoundry/ibm-service->

[science-management-engineering](#)

[LWF] 李文法，孙铁，王卫东，探析网络安全态势感知，绿盟技术内刊，2010年四期，总第11期

[LXP] 李鸿培，信誉技术在安全领域中的应用，绿盟技术内刊，2011年第一期，总第12期

[NewSchool] Adam Shostack, Andrew Stewart, "The New School of Information Security", Addison-Wesley, 2008

[SOA] [http://en.wikipedia.org/wiki/Service-oriented\\_architecture](http://en.wikipedia.org/wiki/Service-oriented_architecture)

[SOC] <http://www.darkreading.com/security/security-management/228300332/soc-2-0-a-crystal-ball-glimpse-of-the-next-generation-security-operations-center.html>

[SOSA] Cristian Aurel OPINCARU, Service Oriented Security Architecture - applied to Spatial Data Infrastructures, Doctoral Dissertation, 2008

[WBF] 吴伯凡，<http://finance.sina.com.cn/leadership/20110523/15499884461.shtml>

[WWD] 王卫东，网络安全态势感知体系探讨，绿盟技术内刊，2011年第一期，总第12期

[ZL1] 赵粮，中国网络安全发展十年，绿盟技术内刊，2010年第一期，总第6期

[ZL2] 赵粮，2010年安全回顾，绿盟技术内刊，2011年第一期，总第12期

# 网络钓鱼产业链分析

技术支持中心 谭荆利

**摘要：**目前一些传统的犯罪形式正逐渐演化，成为形式更加多样、影响范围更广、更加容易逃避追查的新型犯罪形式。在这些犯罪形式中，网络钓鱼无疑是最重要的一员。本文将根据一些典型的网络钓鱼案例，以及各新闻媒体对网络钓鱼事件及防范措施的报道，结合作者所在单位的相关研究数据，来总结网络钓鱼的常见形态、受害人群及主要的防范措施，并尝试挖掘相关黑色产业链的运作模式。

**关键字：**网络钓鱼 钓鱼产业 黑色产业链分析 反钓鱼技术

## 引言

**要**说 2011 年上半年哪些安全事件最能引起我们的注意，莫过于年初曝光的专门针对中国银行网上银行系统的钓鱼事件。钓鱼者通过一个成本低廉的简陋钓鱼网站以及平均不足 1 毛钱 / 条的手机短信，在极短的时间内给网上银行用户带来了出乎意料的巨大损失。来自《新消息报》的消息称：据金山网络云安全中心统计数据显示，这起事件给网上银行用户造成的损

失或已近亿元。另一个与钓鱼相关的事件要数 3.10 特大跨境电信诈骗案了，这起案件虽然表面上与互联网扯不上关系，但事实上它也利用了互联网衍生出来的新事物——IP 电话。

在 Google 上输入“网络钓鱼 事件”关键字，我们可以得到超过 1500 万条搜索结果，即使过滤掉所有重复的记录，最终的数字也是非常惊人的。然而我们不知道的是，搜索结果仅能罗列一些已经曝光的钓鱼事

件，事实上还有很多的网络钓鱼被淹没在互联网的汪洋大海之中。我们对互联网上出现过的各类钓鱼站点进行了收集和分析，根据我们的观察，大概可以将网络钓鱼分为三大类。

## 一、网络钓鱼的方式

### (一)、门户仿冒

通过仿冒被钓鱼的网站（一般为银行、网上商城、支付平台等），诱使受害者访问，以记录受害者的账号、密码等私人信息。此

类钓鱼往往会通过短信通知、在搜索引擎中提高搜索排名等手段来向受害人群扩散。

此类事件中比较典型的有仿冒中国银行网上银行、仿冒淘宝商城、仿冒网易一卡通支付平台、仿冒南航订票网站等。

## (二)、伪造中奖

通过伪造一些流行活动的中奖及领奖工作来实施钓鱼，诱使受害者提供个人信息（姓名、联系地址、身份证、银行账号等）、汇款给特定账号等。此类钓鱼一般通过群发邮件、利用即时通讯客户端（IM）发送消息来吸引受害人群的注意力。

此类事件比较典型的有 QQ 十周年、SOHU 邮箱中奖、非常 6+1 抽奖等。

## (三)、其它方式

还有一些其它形式的钓鱼行为，由于其受害人群相对较小，统一归入此类，其中包括：

### 1、假冒虚拟物品交易

钓鱼者通过构建虚假虚拟物品交易平台，吸引受害者输入机密信息，从而有机会盗取受害者账户中的虚拟物品，转手以谋取利益。

此类事件中比较典型的有游戏物品交易、Q 币交易、六合彩等。

### 2、新奇特物品销售

钓鱼者通过构建虚假新奇特物品购物网站，利用受害者对一些新奇特物品的好奇心和需求来套取其个人信息，利用其信息进一步实时钓鱼。

此类事件中比较典型的有减肥药、透视眼镜、保健品等。

### 3、虚假应用程序

钓鱼者搭建一些虚假的互联网流行应用程序网站，吸引受害者访问，受害者若从这类网站下载程序并运行，计算机就可能会被植入木马程序，导致计算机遭钓鱼者控制或个人信息的泄露等。

此类事件中较典型的有虚假视频网站、虚假游戏外挂网站、虚假程序下载网站等。

### 4、虚假证件

钓鱼者搭建一些虚假的证件在线查询网站或办理各类证件的宣传网站，吸引受害者办理证件，然后提供虚假的证件信息供受害者查询，以骗取受害者资金。

此类事件中较典型的有虚假学信网等。

通过对近年来发生的各类网络钓鱼事件

进行观察和分析，虽然网络钓鱼的形态各有不同，并且钓鱼的目标人群也存在或多或少的差异，但还是让我们发现了他们的许多共同的特征。这些特征直接影响着整个黑色产业链的变革和发展。

## 二、网络钓鱼的特点

### (一)、经济利益为源动力

随着经济的市场化，经济利益已经成为越来越多事物发展的根本动力。受经济利益的驱使，某些利益集团往往会罔顾法律准绳，投入到钓鱼这种投入低廉、但回报丰厚的黑色产业链中来。

### (二)、跨地域协同作案

在警方侦破的多起钓鱼案件中，涉案人员都不在少数，最多的甚至高达 500 多人。从 3.10 案件我们可以看到，在一个钓鱼犯罪团伙中，成员可能来自不同的国家或地区，每个人在团伙中的职责也不尽相同。

### (三)、受害人群针对性较强

钓鱼者通常都有着明确的目标，他们不会无的放矢。在前面的中国银行钓鱼事件中，虽然钓鱼者利用了手机短信来广撒网，但

最终的受害群体却只能是中国银行网上银行的用户。在其它一些钓鱼事件中，也都有着类似的针对性。如：QQ 钓鱼、网易邮箱中奖、非常 6+1 中奖分别针对 QQ 用户、网易邮箱用户和非常 6+1 节目的观众。

**(四)、充分利用高科技手段**

随着科技的进步，网络钓鱼的方式也在随之变化，一些便民的技术手段往往会被钓鱼者利用，成为钓鱼者传播信息的媒介、伪造身份的工具、躲避追查的壁垒。例如：在网上银行钓鱼事件中，钓鱼者需要使用手机短信来传播钓鱼信息；电信诈骗案中，钓鱼者利用 IP 电话伪造来电号码显示等。

从已知的大部分钓鱼事件来看，钓鱼者通常会假冒一个知名企业单位（或组织），通过利用受害者与受害单位之间的信任关系来套取受害者的私密信息甚至是资金。显而易见，大部分的钓鱼事件都是一项影响钓鱼者、受害单位、受害个人三个方面的活动。

**三、网络钓鱼的受害者**

**(一)、受害单位**

根据我们的分析，网络钓鱼的受害单位多集中于一些知名度较高的行业或单位，而钓鱼行为的目标也是指向受害单位的庞大客户群体。

**1、金融**

包括银行、证券公司和第三方支付机构等。

**2、互联网**

包括门户网站、流行应用(如: IM、邮箱等)、网上商城、网络游戏等。

**3、电视节目**

包括非常 6+1、非诚勿扰等。

**4、其它**

包括航空公司、酒店等。

根据我们获取的 184 个样本分析，针对各类客户的钓鱼情况大致分布如图 1 所示。

**(二)、受害人群**

众所周知，80 年代左右出生的人见证了中国互联网的成长，是与互联网融合得最为紧密的一代人。在我们提取的 184 个受害者样本中，40 岁以下的受害者占据了 91% 的份额。其中，有 87 个样本来自于 21~30 岁这个年龄段，占总数的 47%；其次为 20 岁以下的样本，占 25%。

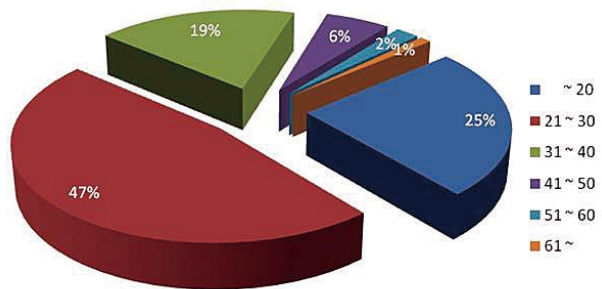


图 1 受害人群的年龄分布

我们可以想象，当钓鱼者确定了钓鱼的目标群体之后，首先需要架设自己的钓鱼网站，然后通过一定的渠道（可能是手机短信、电子邮件等）来发布钓鱼信息，之后等待受害者上钩，从而坐收渔利。在整个过程中，钓鱼网站的架设是技术性最强、且比较耗时的一个环节，它经过拆分后又包括网站建设、空间租用、网站部署等步骤。

根据我们的观察，一个钓鱼网站的生命周期非常短，通常不会超过两周时间，有的甚至更短。如果钓鱼者将主要的精力消耗在架设钓鱼网站上，就很难保证整个钓鱼攻击流程的快速运转。因此，钓鱼者必需借助第三方的机构或人员来承担钓鱼网站的架设等相关工作，而这些工作，通常都由一些空间代理商和平台提供商来完成。

#### 四、产业链

##### （一）、空间代理商

###### 1、采用国外服务器

在我们分析的样本中，绝大多数钓鱼网站的服务器位于美国、欧洲、澳大利亚、韩国和香港等地，这些国外服务器均由国内的空间代理商租用并向外提供空间服务。由于国内监管机构要对国外的网站进行处理，只能通过国外监管机构的实现，而这个沟通协商的过程，时间上难以保证。因此，钓鱼者可以利用这个时间差来有效延长钓鱼网站的生命周期。

###### 2、低价吸引合法网站入驻

空间代理商代理往往用低廉的价格吸引合法网站进驻国外服务器，这从一定程度上掩护了钓鱼网站，防止钓鱼站点被监管机构封锁 IP 地址。

美国全能型主机详细对比								
型号	美国全能100型	美国全能200型	美国全能300型	美国1G入门型	美国1G门户型	美国2G豪华型	美国全能3G型	美国全能5G型
月付价格(元)	-	24	36	42	54	72	84	120
年付价格(元)	100	200 节省30%	260 节省40%	350 节省30%	450 节省30%	600 节省30%	700 节省30%	1000 节省30%
优惠	一次性买两年再享9折优惠，买三年8折优惠							
购买	<a href="#">去购买</a>	<a href="#">去购买</a>	<a href="#">去购买</a>	<a href="#">去购买</a>	<a href="#">去购买</a>	<a href="#">去购买</a>	<a href="#">去购买</a>	<a href="#">去购买</a>
主机配置								
机房线路	美国加州高速机房(圣安娜)							
IP地址	一个							
服务支持	400免费电话支持、售后服务单24小时支持、QQ在线14小时支持、Email支持							
域名绑定	可自由绑定10个域名，让10个域名访问同一空间							
二级域名	赠送免费的二级域名							
退款保证	30天无条件退款							

图2 国外虚拟主机的价格

##### （二）、平台提供商

根据我们的分析，很多钓鱼网站的建设和维护是由专门的团体来负责的，我们称之为平台提供商。平台提供商除了承接钓鱼网站的建设和维护外，也可以为企业或个人提供建站服务。平台提供商的钓鱼站建设已经实现流程化管理，价格低廉。

个人版：首月180元，续费150元/月，单一后台登入模式，全区可以钓，无开区，出租功能！350元=半年 420元=一年。TK域名不收费，使用COM域名+55元 [在线QQ管理](#)

出租版：首月220元，续费180元/月，后台可添加单区用户，可设置用户 [QQ留言](#) 间，信息完美备份，有效防止误删，错删等情况！350元=两个月 [QQ留言](#)

外挂版：假外挂钓鱼，首月180元/月，续费180元。后台过滤重复。

包年版：首月668元，一年中可以随便更换任何游戏，每次更换收取50元手工费。

所有箱子域名费用另算：TK的5元，COM的55元，CN120元。换域名同价，不准拖欠，立给立换！

图3 钓鱼网站建站价格

##### （三）、网络钓鱼者

空间代理商、平台提供商仅仅为网络钓鱼提供了温床和武器，真正的钓鱼活动是由网络钓鱼者来实施的。钓鱼者首要的任务是通

过各种渠道来散播钓鱼网站的信息，吸引受害者访问，主要有以下几种途径：

传播途径	适用场合
手机短信	金融类钓鱼，多见于网上银行钓鱼。
即时消息	互联网类钓鱼，多见于IM中奖钓鱼。
电子邮件	互联网类钓鱼，多见于电子邮箱、电视节目中中奖钓鱼。
搜索引擎	金融类、门户仿冒类钓鱼，多见于网上银行钓鱼、假航空公司网站。
植入广告	互联网类钓鱼，多见于网络游戏外挂、中奖钓鱼。

表 1 钓鱼网站传播途径

由于网络钓鱼者是通过互联网来实施攻击的，基于互联网缺乏有效监管的特性，要对钓鱼者进行跟踪追查是非常困难的。

#### (四)、网外钓鱼者

网外钓鱼者即我们所说的诈骗者，前面曾经提到的电信诈骗案就是由网外钓鱼者实施的。网外钓鱼者通过一定的途径获得大量的用户信息，这些信息极有可能来自网络钓鱼者或一些既得利益集团。通过手工掌握的信息，再使用一些社会工程学的方法，通过电话、邮件等媒介或直接面谈的方式来对既定目标实施攻击。由于社会工程学方法是针对人的心理弱点展开的攻击，比一般的攻击更加难以防范。

但是，由于网外钓鱼者与受害者之间的距离更加接近，这也导致了网外钓鱼者相对容易暴露，所承担的风险自然远远高于网络钓鱼者。相信近几年网络钓鱼的蓬勃发展也与钓鱼者的风险趋避心理有一定的关系。

种子因为有了合适的土壤才会生根发芽，因为有了互联网这片土壤和亿万网民提供的养分，网络钓鱼黑色产业才能在近几年急速膨胀。要有效避免网络钓鱼对互联网的危害，不是一朝一夕就能够完成的，而是需要全体网民不断地提高自身的安全意识、各企事业单位做好安全防范工作以及国家监管机构加强互联网监管力度。

## 五、网络钓鱼防范措施

### (一)、单位方面

受害单位是指那些受网络钓鱼影响的单位，通常为各类金融机构、门户网站、网络购物平台等。很多单位都曾经受到钓鱼攻击的影响，不仅给用户带来了经济上的损失，同时也对自身的声誉产生一定的负面影响。因此，目前绝大部分单位在提供业务服务时都会提供一种以上的防范措施。常见的防范措施有三种：

#### 1、宣传教育

常发生钓鱼事件的客户通常都会在其网站显要位置张贴公告，罗列一些典型的钓鱼事件，提醒其用户注意可能发生的各种安全问题，提高用户的风险防范意识。有些客户甚至会提供一些安全意识方面的培训、评级等。

#### 2、技术手段

钓鱼攻击影响最大的通常是用户的资金安全，所以影响最大的多为用户的银行账户，以往银行机构提供的账号安全的保护措施，部分对钓鱼攻击还是有作用的，例如 U 盾（数字证书）。而诸如短信确认、一次一密、浏览器口令控件等方式则无法有效地防止钓鱼攻击。

#### 3、第三方监控

一些安全公司具备监控钓鱼网站的技术能力，被钓鱼客户可以委托他们来监控针对其业务的钓鱼活动，及时发现并处理，从而将风险降到最低。

## (二)、个人方面

对于普通个人来说，要想有效避免遭受网络钓鱼攻击，至少需要做到以下几点：

### 1、丰富安全知识

多关注新闻动态、常用业务安全现状、流行安全事件等，提高自身的安全知识和行为意识。

### 2、擦亮眼睛

钓鱼者通常使用一些模糊手段来混淆网民们的视听，如相似的域名、邮箱、电话、网站风格等。只要仔细辨别，总能发现钓鱼者与正规业务之间的区别。

### 3、不贪小便宜

对于一些来历不明的中奖、购物等信息不理睬，更不去访问所提供的链接。

### 4、更新业务软件

业务的提供者为了保证业务的安全，总会不定期更新业务软件，增强其安全功能。只有及时更新了业务软件才能有效防止安全问题的发生。

### 5、记住业务网站域名

很多人喜欢使用搜索引擎来搜索某个业务站点，这是一个不太好的习惯。钓鱼者使用的比较普遍的一种方式就是通过提高搜索排名来实施钓鱼攻击，所以不要简单地认为排名靠前的就是正确的门户网站。记住办理业务的网站域名，在使用时直接输入地址栏后访问是一个不错的习惯，虽然它可能导致你使用时不太方便。

## (三)、政府监管机构

对于钓鱼攻击的监管，监管机构采用的主要方式是客户举报后查封，方式较为被动，不能有效地遏制钓鱼攻击。目前的主要监管措施包括以下几种：

### 1、查封网站空间

监管机构可以通过协调空间提供商来查封钓鱼者的网站空间，使钓鱼网站失效。但钓鱼者可以通过将空间放到国外服务器，来增加查封空间的时间成本。

### 2、查封 IP 地址

监管机构也可以通过查封钓鱼网站所在的 IP 地址来快速封锁钓鱼站点。但钓鱼者

可以将钓鱼站点与合法站点混合放在同一个 IP 地址上，使监管机构无法直接查封。

### 3、查封域名

对于申请了特定域名的钓鱼网站，监管机构可以联系域名提供商来封锁其域名，达到封锁钓鱼网站的效果。但钓鱼者可以使用国际域名、国际二级域名来增加查封域名的时间成本。

### 4、跟踪、监视

公安机关一般会采用跟踪、监视等手段来追踪一个钓鱼者的账户资金动向，以确定钓鱼者所在的位置。但钓鱼者通常采用异地多账户多人操作的方式来进行资金流动，使公安机关无法进行跟踪定位。

只有单位、个人和监管机构之间通力合作，才能真正有效地防范网络钓鱼攻击。

## 参考文献

- 新消息报，2011，中行网银频遭“钓鱼”
- 经济参考报，2011，电信诈骗现专业服务产业链
- 21 世纪网，2011，金融网络欺诈大调查

# 攻击者想要什么

研究部 颜涛

**摘要：**本文主要介绍了2011年上半年三个影响较大的攻击事件，分析了这三个事件的起因、攻击过程以及所造成的影响。通过从攻击者的角度分析攻击来源、所采用的技术和他们的最终目的，从而有针对性的采取相应的防御策略，将攻击所造成的损失降到最低。

**关键词：**马来西亚 DDoS 事件 索尼 PSN 信息泄露事件 RSA SecurID 泄露事件 anonymous LulzSec

## 一、介绍

2011年上半年，各种攻击事件依然层出不穷，并发生了互联网历史上最大的信息泄露事件，给企业、政府和一些大型机构造成了严重的损失。随着网络应用越来越复杂，网络规模越来越大，互联网的安全也承受着越来越大的考验。这些攻击者都是谁？他们采用了何种攻击手段？攻击者想要什么？所谓知己知彼，百战不殆，知道了这些问题，使得防御者们对症下药，在最大程度上减少甚至避免这些攻击事件的发生。本文分析了2011年上半年3个影响较大的攻击事件，并从攻击者的角度分析了事件的前因后果以及所能采取的策略。

## 二、马来西亚 DDoS 事件分析

### (一)、事件原因

anonymous 声称要入侵马来西亚网站 ([www.malaysia.gov.my](http://www.malaysia.gov.my))，并命名此次攻击为“马来西亚行动”(operation malaysia)。这则消息以图片的形式在 <http://i.imgur.com/PTFWh.png> 网站上登出。如图1所示。



图1 operation malaysia

之后 anonymous 又在 youtube 上发布了一个视频，公布了攻击马来西亚政府网站的原因。最主要是对政府网络审查制度的不满(马来西亚政府封禁了包括 wikileaks 在内的 10 个站点)以及日前关闭多家免费网络资源共享网站。声明如下：



Greetings, Malaysia,

We have seen the censorship taken by the Malaysian government, blocking sites like The Pirate Bay, and WikiLeaks. Malaysia is one of the world's strictest governments, even blocking out movies, and television shows. These acts of censorship are inexcusable. You are taking away a basic human right. The internet is here for freedom, without fear of government interference. Do not think that no one else notices. Your structured government has done the talking, and we hear loud and clear. Let this be an announcement to all your people. This is a sign, a warning, and an opportunity to listen to ideas above your own. In a way you are being stubborn. But how will this help anyone or your country. We fear that if you make further decisions to take away human freedom. We are obligated to act fast and have no mercy. For rules were meant to be broken. And corruption was meant to be washed away and forgiven. Now we will wash your corruption away so be prepared. Take this as a favor.

We are Anonymous.

We are Legion.

We do not forgive.

We do not forget.

Expect Us.

此后 anonymous 在 twitter 上招募攻击者并提供 DDoS 工具 LOIC 的下载。

## (二)、事件结果

经马来西亚通信与多媒体委员会证实，51 个政府网站遭到了攻击，其中 41 个网站不同程度受损。被攻击的网站主要是马来西亚政府门户网站、信息部网站、火险和应急服务部门等政府机构网站。攻击的手段对于大多数网站都采用了 DDoS 的方式，很多网站被迫关闭或因 DDoS 不能访问。有部分网站被篡改，极个别网站资料被泄露。部分结果如图 2、图 3 所示。



Malaysia Official Government Website [\[link\]](#) – [Down]

- SabahTourism.com [\[link\]](#) [Hacked][Leaked]
- CIDB [\[link\]](#) [Hacked] [Up]
- Land Public Transport Commision [\[link\]](#) [Suspected]
- Malaysian Meteorological Service [\[link\]](#) [Down]
- ASEANconnect [\[link\]](#) [Suspected]
- Hollywood-Artist.info [\[link\]](#) [Suspected]
- Ministry of Education [\[link\]](#) [Down]
- Suruhanjaya Pilihanraya Malaysia [\[link\]](#) [Down]
- Bomba [\[link\]](#)[Down]
- TMNet [\[link\]](#) [Down]
- Perbendaharaan Malaysia [\[link\]](#) [Down]
- Kementerian Kerja Raya Malaysia [\[link\]](#) [Down]
- Parlimen Malaysia [\[link\]](#) [Down]
- JobsMalaysia [\[link\]](#) [Down]
- Kementerian Penerangan, Komunikasi dan Kebudayaan [\[link\]](#) [Down]

图 2 被攻击网站结果

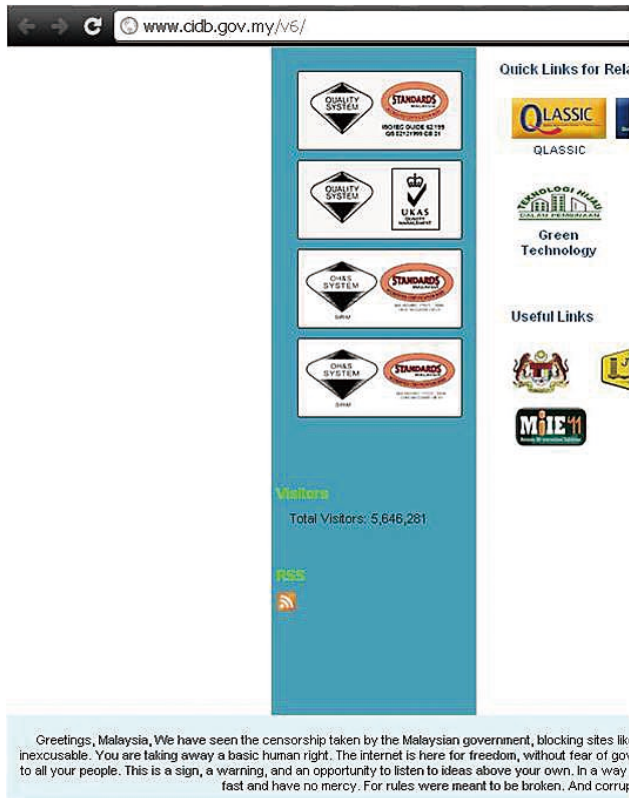


图 3 www.cidb.gov.my 网站被篡改结果

与此同时，马来西亚国内的一些独立的黑客组织和个人也参与了此次的攻击。jpm.gov.my，其网站敏感信息包括用户名密码遭到了泄露，如图 4 所示。

值得一提的是一个叫做 dragon force 的马来西亚当地的黑客组织，他们配合 anonymous 篡改了不少马来西亚的政府网站。链接如

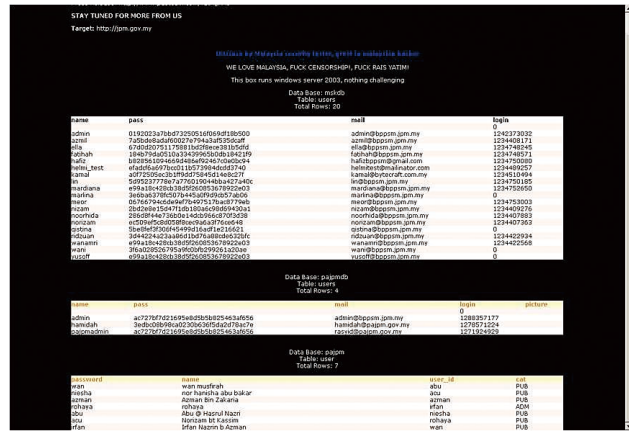


图 4 jpm.gov.my 信息泄露截图  
(来自 <http://pastethtml.com/view/axb1rno03.html>)

下：<http://mydragonforce.wordpress.com/>。

其中受损最严重的网站是马来西亚沙巴旅游网 [www.sabahtourism.com](http://www.sabahtourism.com)。其有些网页被攻击者删除，根据 anonymous 发布的结果来看，攻击者获得了服务器的最高权限，并且获得了网站的全部数据（包括 3400 多个用户信息），并在网站上公布了 300 多个用户名、邮箱、密码等信息。

(三)、事件分析

anonymous 是一个分散的团体，此次攻击大多数是马来西亚国内的 anonymous 成员或独立黑客组织，其运用的最主要手段还是 DDos，运用的工具是 LOIC。绝大多数网站遭到了拒绝服务攻击，有少部分网站遭到了篡改，有极个别网站信息遭到了泄露。据相关安全研究员分析，类似于黑洞这种类型的 ADS 完全能够防御此类的

DDoS 攻击。根据被篡改的网站得到的信息，除了沙巴旅游网攻击者并没有得到服务器系统的最高权限，而沙巴旅游网由于是 mysql 和 php，如果存在注入点就有可能读出 /etc/passwd、/etc/shadow 等敏感文件或通过各种手段提升权限从而获得系统的最高权限。由于没有资料表明攻击者到底使用了哪一种手段，根据其发布的信息的格式来看，很可能是通过 web 入口进行攻击，比如通过 SQL 注入读取数据库数据。从这个角度来说，一些安全设备比如网络防篡改系统和网络应用防火墙就可以成功抵御此类攻击。

### 三、Sony PlayStation Network 信息泄露事件分析

#### (一)、事件起因

2011 年 1 月，George Hotz 发布了破解 PS3 的 Root Key，玩家可以在 PS3 上运行任何破解的游戏和代码，之后索尼以 Hotz 违反《数字千年版权法案》(Digital Millennium Copyright Act) 和《计算机欺诈与滥用法案》(Computer Fraud Abuse Act) 为由起诉；通过法院，索尼得到了 Hotz 在 Paypal 的账户信息、所有访问 geohot.com 网站的用户 IP，还试图让 Youtube 交出所有看过 Hotz 上传视频的网民的 IP 地址。索尼对此事件的态度可能不是索尼受到攻击的最主要原因，但很可能是一个导火索。

#### (二)、事件过程和结果

2011 年 4 月，Anonymous 组织入侵了索尼的一个网站，写上了“Congratulations, Sony. You now have now received the undivided attention of Anonymous. Your recent legal action against our follow hackers, Geohot and Graf\_Chokolo, has not only alarmed

us, it has been deemed wholly unforgivable.” 如图 5 所示。

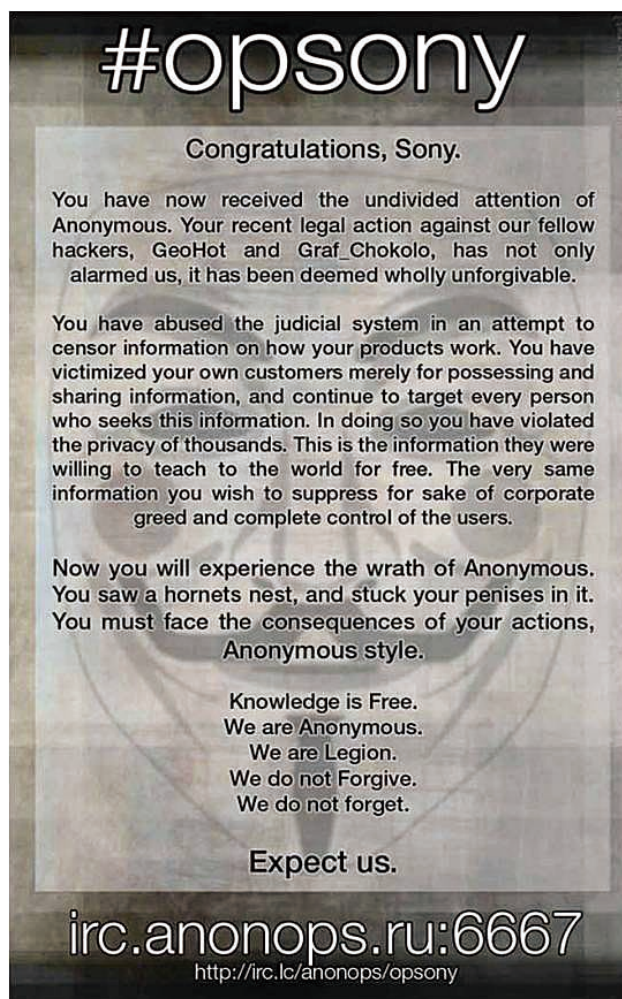


图 5 anonymous 入侵索尼某网站宣言

之后，Anonymous 又对 Sony PlayStation Network 和其一些网站进行了 DDoS 攻击。但这些攻击对 Sony 的网络运行并没有造成实质性的威胁和损失。2011 年 4 月 26 日下午在索尼北美的 Blog 上，索尼承认在 4 月 17 日和 19 日之间，PS3 网络遭到攻击。调查组花了一个星期时间调查之后才发现 7 千万 PS Network 和 Qriocity 音乐服务的用户个人信息被黑客盗走。被盗走的个人信息包括：姓名，地址（门牌号，城市，邮编，国家），email，出生日期，PlayStation Network/Qriocity 的用户名和密码，handle/PSN online 用户名。被盗的账户分布如图 6 所示。还有用户在 PlayStation 网的购买历史记录，账单地址，账号安全问题答案。索尼声称还没有看到用户信用卡信息被盗的迹象，但不可排除被盗的可能。在给美国国会的信件中，索尼还解释说，索尼 PSN 后台包括 130 台服务器以及 50 个应用软件，大约有 10 台服务器被黑，而公司确认系统被黑用了数日。消息发布之后，对索尼公司的网络攻击出现了堆积效应，索尼在线娱乐系统的服务器也被攻击，服务器上共有 2460 万名用户的信息，包括姓名、地址以及密码，以及 12700 张非美国本土的信用卡号以及到期日期，除此之外入侵者还获得了大概 10700 份来自德国、奥地利、荷兰以及西班牙等地区的订阅用户直接支付记录。其后，索尼遭遇到大大小小的黑客攻击 10 余次，包括索尼影视 (Sony Pictures)、索尼欧洲 (Sony Europe)、索尼希腊 BMG 网站 (Sony BMG Greece)、索尼泰国 (Sony Thailand)、索尼日本音乐 (Sony Music Japan)、索尼爱立信加拿大 (Sony Ericson Canada) 等等。值得注意的是 lulzSec 组织，它不但宣称对某些攻击负责，并且透

露攻击过程、发布获得的数据库信息甚至是网站的源代码 (Sony

**EXHIBIT B**  
**PlayStation®Network Services Countries / Regions and Accounts**

Countries/Regions	Accounts	Countries/Regions	Accounts
Argentina	101,269	Luxembourg	37,457
Australia	1,560,791	Malaysia	88,999
Austria	412,233	Malta	15,144
Bahrain	26,392	Mexico	957,543
Belgium	669,155	Netherlands	1,135,134
Brazil	448,835	New Zealand	235,209
Bulgaria	78,017	Norway	550,068
Canada	3,524,227	Oman	9,801
Chile	80,357	Peru	35,517
Colombia	91,246	Poland	376,298
Croatia	33,578	Portugal	643,815
Cyprus	21,367	Qatar	46,164
Czech Republic	90,878	Romania	32,695
Denmark	383,033	Russian Federation	444,990
Finland	336,024	Saudi Arabia	651,018
France	4,701,424	Singapore	167,517
Germany	3,233,800	Slovak Republic	18,563
Great Britain	9,296,317	Slovenia	16,384
Greece	210,459	South Korea	235,041
Hong Kong	897,174	Spain	2,982,592
Hungary	29,371	Sweden	534,365
Iceland	20,858	Switzerland	431,930
India	89,258	Taiwan	255,518
Indonesia	24,990	Thailand	30,877
Ireland	436,158	Turkey	145,000
Israel	45,335	Ukraine	5,898
Italy	1,473,187	United Arab Emirates	254,820
Japan	7,427,038	United States	31,140,307
Kuwait	93,453	South Africa	102,443
Lebanon	21,309		

图 6 索尼 PSN 账户分布

Computer Entertainment Developer Network 的源代码就被其公布在网上)。它声称利用 SQL 注入攻击获得了sonypictures.com, sonybmg.nl 和 sonybmg.be 的数据库。数据库包含了超过 100 万索尼美国、荷兰和比利时客户的个人信息, 包括明文存储的密码、电子邮件、家庭地址、邮编、出生日期。

### (三)、事件分析

此次针对索尼 PSN 网络及其相关服务的攻击泄露了索尼超过 1 亿的用户数据, 一千多万的信用卡信息, 给索尼造成关闭 PlayStation Network 等网络、聘请数家计算机安全公司调查攻击情况、重建安全系统、游戏用户赔偿等显性损失就达几亿美元, 更不必说股票下跌, 失去信任等隐性损失。曾有日本美容企业因顾客信息外泄, 结果被法院判令向每名顾客赔偿 3 万日元。如果按此标准, 索尼面临的赔偿额可能达 2 万亿日元 (245 亿美元)。

分析这一系列的攻击来源, 除了 anonymous 组织在前期针对索尼进行了一些 DDoS 攻击和后期 lulzSec 宣布对某些网站负责之外, 从索尼召开的 PSN 事件说明会来看, 还没有确切证据定位攻击源。先前 Anonymous 组织宣称与 PSN 网络被入侵无关, 而以 lulzSec 的一贯风格来看, 如果是他们入侵了 PSN 网络, 大张旗鼓的宣扬是免不了的。由此来看, 入侵 PSN 网络另有其人, 之前索尼请 FBI 来查证时说过可能是两个组织配合攻击, 称自己是一次大规模黑客攻击事件的受害者, 此次攻击源自“非常专业、异常复杂”的犯罪组织, 目的是盗取个人和信用卡信息。但这样说免不了逃脱责任隐瞒大众之嫌。至于真实的攻击目的, 以及得到的用户数据及信用卡信息是否

流入黑市, 却不得而知。

从攻击手段上来说, 爱出风头的 anonymous 组织和 lulzSec 组织在此次攻击中使用 SQL 注入和本地文件包含漏洞利用, 以及利用僵尸网络发动 DDoS 攻击。而针对 PSN 网络进行的“入侵 10 个服务器, 长达数日”的攻击所采用的手段以及利用的漏洞, 索尼方面均含糊其辞, 语焉不详。坊间流传着两种说法, 一是通过 SQL 注入攻击 PSN 应用程序, 二是数据库服务器可能被公开访问。如图 7 所示。

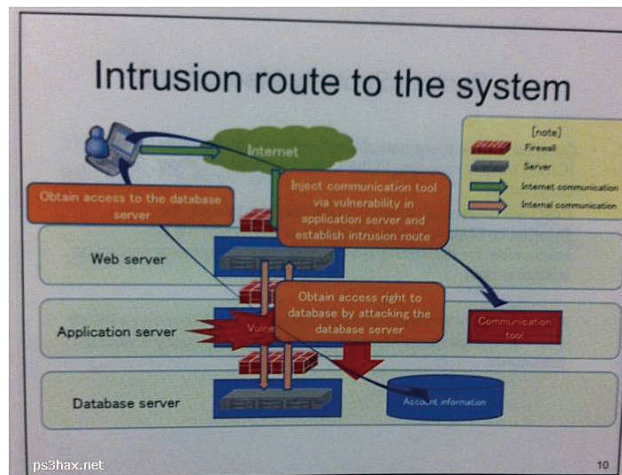


图 7 索尼 PSN 被攻击的路径

而索尼方面也表示, “黑客是通过一个已知的系统软件漏洞进入了服务器”, 不过 SNEI (Sony Network Entertainment Inc.) 的管理人员并没有注意到这点。比较可信的一个说法是由于 PSN 所用的 redhat 系统中的 apache 服务器没有及时更新安全补丁, 从而使黑

客成功入侵到内网。而入侵的原因似乎和游戏有关。具体来源如图 8 所示:

Their PS3 cluster computers are very good because linux/unix is the best for servers, only problem is updating the OS on 2200 PS3's in one cluster, takes some time and employees. But do-able for something important like PSN. That is if you take your customers serious...

I don't like updating Windows because all of their crap but I always install their latest security patches. And for one reason: By publishing the vulnerabilities the leaks are known by everyone who wants to misuse security holes.

```
[user12] i also know that the server that does the x-5 tickets is a bit more tight about the ciphers than any other system in sonyland.
[user12] if sony is watching this channel they should know that running an older version of apache on a sony server with known vulnerabilities is not wise, especially when that server freely reports its version and its the auth server.
[user12] its not old version, they just didnt update the banner.
[user12] i consider apache 2.2.15 old.
[user2] which server.
[user12] it also has known vulnerabilities.
[user2] outh.np.ac.playstation.net.
[user2] yes the displayed version u see via banner is not the real version.
[user12] unless they updated it in the last couple weeks.
[user12] i doubt that since its not trivial to change that.
[user12] its a bit more invasive than just setting it to Prod like they do on their other servers.
[user11] you know, watching this conversation makes me think about whether it was a good idea after all to buy a couple of games from ggg using a visa card.
[user2] its just backported security patches.
[user11] i did remove all my info after downloading the games though.
[user12] that is just ggg, not the store.
[user12] they are running linux 2.6.9-2.6.24 on that box too.
[user12] that too is old.
[user2] lol @ buying on store.
[user11] yes, but their general attitude towards security just seems...ugh.
[user2] sony wont misuse the info i bet xD.
[user2] but just prevent using ciphers of unknown ggl.
[user2] even better from ALL ggl.
[user2] make it own lol.
[user12] so i doubt that they are spoofing the network stack on that box as well.
```

```
[user12] my guess is that it really is undmaintained "it works why change anything".
[user2] could be.
[user12] sony really should update that stuff to something more current.
[user2] yes.
[user2] but imagine.
[user2] sony == 45 environments.
[user2] and for example.
[user2] every ggg has 50 subdomains.
[user2] to external machines.
[user2] its like huge.
[user2] who wants to do this xD.
[user2] ggl = lazy.
[user2] wont change.
```

图 8 黑客在聊天室中讨论索尼 PSN redhat 系统 apache 服务器漏洞

另外, 从用户密码都以明文或者简单的 hash 存储 (没有加密) 以及大量网站暴露出的 SQL 注入漏洞来看, 索尼 PSN 网络的安全性以及其管理员的安全意识并不足以阻止网络中的一些简单攻击。

究其原因, 索尼似乎更喜欢用法律手段来解决其服务器被入侵的安全问题, 而忽略自身的安全问题或者不注重企业的安全体系建设。索尼此次暴露出的安全问题值得其他企业引以为鉴。

#### 四、RSA SecurID 泄露事件分析

##### (一)、事件过程及结果

RSA 是 EMC 公司的安全部门。2011 年 3 月, RSA 在网站上发表声明称, 有人以 APT (Advanced Persistent Threat) 方式对 RSA 发起相当复杂的网络攻击, 与 SecurID 技术相关的数据遭窃取, 但数据泄露的程度以及攻击者所采取的攻击方式, RSA 拒绝透露更多信息。APT 攻击经常用于间谍活动, 其攻击目标是公司或政府部

门内部的源代码和其它信息，通常涉及目标网络、关键员工和运营领域的机密，利用多种技巧获悉内部信息如社交工程及软件漏洞的利用。去年 APT 对 Google 及其它公司的攻击就利用了 IE 的 0day 漏洞 (Aurora)，通过邮件向 Google 的内部员工发送含有 0day 漏洞附件或链接的邮件。

## (二)、事件影响

在 RSA 被入侵之后，美国国防巨头洛克希德马丁、诺思罗普格鲁曼和 L-3 Communications (技术与通讯系统制造商) 接连遭黑客攻击，攻击方法如出一辙，都是使用克隆的 RSA SecurID 令牌。最近，RSA Security 宣布替换大约 4000 万 SecurID 令牌。

SecurID 电子令牌，内置了电池和芯片，电池一般可用 2-3 年。芯片与 RSA 认证服务器采用同一种算法，并且与 UTC 时间相关联。电子令牌是通过种子文件 (Token File, XML 文件格式) 导入到 RSA 认证服务器中，在同一个标准时间，令牌所显示的数字与 RSA 认证服务器所计算出来的数字是一致的。

电子令牌第一次使用，需要用户自己来创建一个属于自己的静态密码，称之为 PIN 码，PIN 码会在 RSA 认证服务器上加密保存。当用户创建 PIN 码后，认证的最终过程为：用户的 PIN 码 + 电子令牌显示的动态密码。

SecurID 令牌应用于双重认证系统，每个用户账号连接一个令牌，每个令牌每 30 秒或 60 秒产生一个伪随机数。登录时，用户需输入用户名、PIN 码和令牌产生的伪随机数。认证服务器知道特定令牌所显示的伪随机数，以此确认用户是否持有他们的令牌。伪随

机数的生成算法采用的是 128 位的 AES，每个令牌都有一个不同的初始化种子，这个种子与用户账号相连。128 位的 AES 加密算法本身不会有任何问题，唯一的可能就是攻击者在入侵 RSA 的过程中获取了 SecurID 的初始化种子，因此 SecurID 令牌已经无法保护 RSA 的客户抵御黑客攻击。除了以上三家成了 RSA SecurID 泄露的受害者之外，国际货币基金组织 (IMF) 似乎成了 RSA 最新的受害者。国际货币基金组织检测到一个单一受感染的机器在访问敏感数据。一些分析表明，攻击者可能在攻击过程中的某一步使用了 IMF 员工的 SecurID 密码。

## (三)、事件分析

此次针对 RSA 的攻击使得 RSA 更换了 4000 万个 SecurID 令牌，4 家公司受到不同程度的攻击。起初是由于 RSA 的一名员工从垃圾邮箱文件夹收取了一封鱼叉式网络钓鱼 (Spear-phishing) 的电子邮件，随后打开了附件中一个受感染的 xsl 文件，其中嵌入了一个 flash 的 0day (CVE-2011-0609)。(利用 CVE-2011-0609 进行钓鱼攻击的邮件如图 9 所示。) 攻击者成功植入一个名叫 Poison Ivy remote administration tool (RAT) 的远程控制软件，其做了加壳等处理，使得基于特征码的杀毒软件失效，随后利用此用户的权限开始访问内网的数据库并进行进一步的内网渗透和数据挖掘，找到了含有与 RSA 的 SecurID 认证令牌有关的敏感信息的数据库，并把其上传到某个外网服务器；其后黑客可能又利用钓鱼、木马等手段获取一次用户合法登录信息 (用户名、静态 PIN 码、SecurID 动态口令、UTC 时间等)，通过逆向分析 SecurID 服务

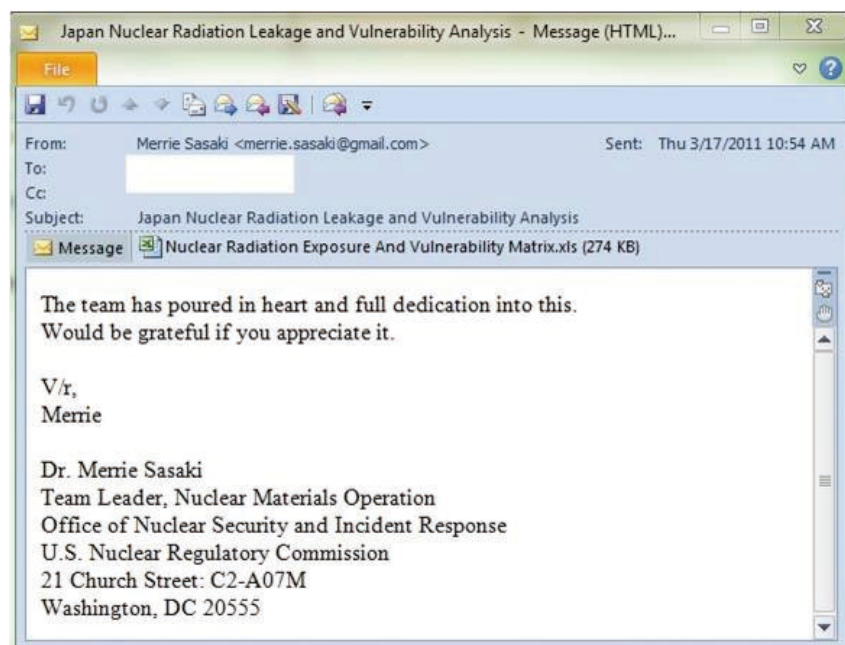


图 9 利用 CVE-2011-0609 进行钓鱼的邮件

端程序及上述获取的用户信息找到用户与 SecurID 令牌种子的对应关系，因为理论上某个 UTC 时间服务端只有一个 SecurID 种子产生的动态口令与用户输入的 SecurID 口令相同，进而伪造合法 RSA 用户（包括美国国防巨头洛克希德马丁、诺思罗普格鲁曼和 L-3 Communications 等）的身份，登录其员工的邮件服务器或者直接登录到

企业内网进行进一步的渗透和攻击。攻击手段和针对 Google 的攻击如出一辙。显然跟 anonymous 和 lulzSec 这些组织使用的攻击技术相比，此次针对 RSA 以及后续利用 SecurID 种子对其他几个公司的攻击手段显得非常专业和隐蔽，也更加难以防范。

## 五、总结

从攻击者来说，攻击马来西亚的 Anonymous 和攻击索尼的 lulzSec 同属一类，他们做事张扬，追求自由平等，常常是因为自由和霸权主义的原因对某些网站或者服务器进行攻击，采用的攻击手段常常是 DDoS 和 web 渗透。而攻击并窃取索尼 PSN 数据的黑客则有着明显的利益倾向，行动也相对隐秘，常常会定点攻击，攻击目标常常是服务器，攻击手段也比较多样，但最主要的还是针对 web 和数据库入口的渗透。而 RSA 的攻击者很有可能是非常专业的组织，他们攻击严密，手段高明而复杂，通常会使用 Oday 漏洞对大型机构、企业或者组织的客户端进行钓鱼或者在机构的网站上用 Oday 漏洞挂马，从而控制重要客户端，然后渗透到企业或者大型机构的内网，用以窃取源代码等机密数据。此类攻击由于其实施难度和对攻击者的要求，在网络中并不常见，近年来也只有 Stuxnet、Aurora、RSA 三个事件的发生。但每次的影响都非常之大，必须提高警惕。总而言之，攻击者想要什么，我们就保护什么，是一个简单而易用的原则。



---

**参考资料**

---

1. 大马政府网站遭黑客入侵 GOV website defaced by Anonymous hacker group  
<http://www.rajauda.com/cn/viewtopic.php?f=76&p=5165>
2. dragon force 官方博客  
<http://mydragonforce.wordpress.com/>
3. Operation Malaysia: Anonymous DDoS attacks cripple gov websites  
<http://www.examiner.com/anonymous-in-national/operation-malaysia-anonymous-ddos-attacks-cripple-gov-websites>
4. 'Anonymous' Hackers Group to attack Malaysia Gov. My Websites #OpMalaysia  
<http://joshuaongys.com/2011/06/anonymous-hackers-group-attack-malaysia-government-gov-my-websites/>
5. Sony PSN 事件说明会重点摘要  
<http://cn.engadget.com/2011/05/01/sony-psn-press-event/>
6. Sony PSN 事件报告书  
<http://gnews.buynow.com.cn/portal.php?mod=view&aid=11754>
7. Sony PlayStation Network 网络服务被攻击——七千万用户资料泄露  
<http://bbs.unnoo.com/forum.php?mod=viewthread&tid=24&romuid=1>
8. lulzSec 网站  
<http://lulzsecurity.com/releases/>
9. 索尼与黑客们的恩怨情仇  
<http://www.cnbeta.com/articles/144250.htm>
10. PSN Accounts Regional Breakdown + How PSN was Hacked (diagram)  
<http://www.ps3hax.net/2011/05/psn-accounts-regional-breakdown/>
11. 索尼被黑 10 余次之谜：黑客借网络入侵炫耀  
<http://www.cnbeta.com/articles/145241.htm>
12. SecurID  
<http://en.wikipedia.org/wiki/SecurID>
13. RSA 网络遭攻击或影响 SecurID 认证  
<http://www.cnetnews.com.cn/2011/0321/2023118.shtml>
14. IMF May Be Latest Victim of RSA SecurID Hack  
<https://www.infosecisland.com/blogview/14400-IMF-May-Be-Latest-Victim-of-RSA-SecurID-Hack.html>
15. RSA Security Attack Timeline  
<http://aggressivevirusdefense.wordpress.com/2011/04/10/rsa-security-attack-timeline>
16. CVE-2011-0609 - Adobe Flash Player ZeroDay - Update  
<http://contagiodump.blogspot.com/2011/03/cve-2011-0609-adobe-flash-player.html>

# 企业移动设备安全管理方法与实践

安全研究院 王卫东

**摘要：**本文首先归纳了移动设备（主要指智能手机和平板电脑等）新的功能特性，分析由新的特性所引入的脆弱性及其对应的安全威胁，从而比较全面的总结了移动设备的安全风险，并参考相关资料总结出移动设备安全管理的最佳实践以及移动设备管理系统的核心功能要求，供企业的 IT 安全管理人员参考。

**关键词：**移动设备安全 移动设备管理 企业设备安全管理 最佳实践

## 1、引言

这里所谓的移动设备主要是指智能手机和平板电脑两大类可以用于移动办公的电子终端设备。随着移动设备的普及，很多企业的员工开始使用这种新型的移动设备作为办公终端。据 Gartner 统计,2010 年第四季度,智能手机(1 亿部)的销量首次超过 PQ 9200 万台),2010 年智能手机增长 72%。2010 年平板电脑的销量 1700 万台, Gartner 预计 2011 年将达 4500 万台。而随着云计算技术和 3G 甚至 4G 无线数据通信服务的广泛应用,更加便携和随时在线的移动设备会更加普及。新型办公终端的引入,为企业内部的信息安全带来了新的挑战。

本文从归纳移动设备的功能特性入手,分析该类设备的安全风险,并在此基础上总结出移动设备安全管理的最佳实践,供企业的 IT 安全管理人员参考。

## 2、移动设备风险分析

### 2.1 移动设备的特性

移动设备在几何尺寸、物理特性、计算能力、应用场景等方面与以往的台式或膝上设备(台式或笔记本电脑)都发生了较大变化。主要体现在:

- 体积小重量轻,更便于携带;
- 持续供电能力相对较低;

- CPU 的计算能力相对较低;
- 具有多种通讯接口, 如 USB、LAN、WIFI、蓝牙、3G 无线数据通讯、GPS 等;
- 在移动的环境中使用;
- 缺少本地的技术支持;
- 操作系统种类繁多, 如 Android、iOS、Symbian、Windows Mobile 等。

## 2.2 移动设备的信息资产

移动设备是个人专用产品, 而且通常有十多种应用在上面运行, 如电话、电子邮件、日程、访问互联网、通讯录、任务管理、消息(文本/图片/视频)、聊天、VPN、文件管理、存储、社交网络、位置服务、移动商务。使用这些应用或服务时, 肯定涉及大量的个人信息, 如: 银行账户、邮件内容、消息内容、账户和密码、联系人信息、网站访问足迹、个人行程安排等等。除此以外, 移动设备上可能还存储与工作相关的文档和数据。

## 2.3 移动设备的脆弱性

移动设备的最主要的特性就是便携性, 因此它的物理安全脆弱性要远比台式设备

高, 很容易遗失或被盗。

移动设备使用的操作系统种类和版本繁多, 很多都存在漏洞。目前移动设备的主流操作系统有 iOS(苹果公司开发的, 基于苹果 OSX 的操作系统) 和 Android(谷歌公司开发的, Linux 和基于 Java 平台的 Dalvik 两种操作系统的结合体)。以 iOS 为例, 从发行到现在共发现了 200 多个漏洞, 其中大部分属于低风险漏洞, 利用这些漏洞, 一般只能取得某个应用程序的控制权限。也有些漏洞可以导致非常严重的问题, 攻击者甚至可以实现对设备的管理员级控制, 这样就可以获取设备中几乎所有的数据和服务。iPad2 的 iOS 越狱行为(获得系统的超级用户权限, 以便随意擦写任何区域的运行状态, 进而安装和运行第三方程序), 是利用浏览器访问越狱网站触发 PDF 字体处理上的缓冲区溢出漏洞, 获得对设备的完全控制。整个越狱过程本质上和黑客攻击的原理完全一致, 只是越狱过程是设备使用者自愿利用漏洞。理论上一个经过越狱的系统, 就是一个证实存在漏洞系统。Android 系统的情况也很类似, 目前已发现 18 个漏

洞中修补了 14 个, 另外未修补的 4 个中只有一个是高危漏洞, 在 Android V2.3 得到修复。但是未升级到 2.3 版本的设备将存在高风险。

移动设备上的通讯接口比固定使用的设备上的通讯接口要多, 因此这些种类繁多的通讯接口都可能成为新的攻击面。而有些通讯没有经过身份认证和加密, 很容易受到攻击。例如, GPS 通讯很容易受到干扰和欺诈。

有些脆弱性是由于系统的配置不当引起的。原则上设备上暂时不用的端口, 应该配置成关闭。例如, 在不使用蓝牙的时候, 应该关闭蓝牙设置。应该配置身份认证选项, 使得系统启动后需要身份认证才能继续使用设备。

## 2.4 针对移动设备的安全威胁

对移动设备的安全威胁, 大致可以分为三大类: 物理威胁、操作系统威胁和网络威胁。

偷盗行为和看管疏忽是针对移动设备物理安全的最大威胁。容易发生设备遗失的场所主要包括: 高等院校、汽车、图书馆、机场、

宾馆和会议中心、办公室、医院。

恶意代码是移动设备的最大威胁，这些恶意代码主要表现为病毒、僵尸程序和间谍软件或三者的混合体。病毒的主要作用是在用户不知道的情况下滥用网络，如拨打高收费电话或发送多媒体短信，以消耗用户的费用，套取非法收益。僵尸程序主要是作为黑客控制被攻陷系统的代理，攻击者可以用来发动拒绝服务攻击。

间谍软件可以用获取系统上的机密信息。例如 2006 年 9 月，有人发现塞班操作系统上运行着一种称为 Acallano 的间谍软件。这种间谍软件把所有收发的短信息导向一个外部的号码。这样就会允许别人安装间谍软件监视受害人的短信流量。2006 年 4 月，一款叫做 Flexispy 的商业软件上市。这款软件可以远程激活设备的麦克风风监控电话内容。尽管这款软件的初衷是用来监控配偶或是不听话的孩子，但也可以作为公司的监听工具。它会在用户不知情的情况下，发送日志信息到中央服务器。黑客也可以藉此访问实体设备安装软件，读取机密的信息，从服务器上检查日志信息，并实施窃听。

这些威胁与台式终端上的完全类似。所不同的是，这些恶意代码的传播途径更加丰富一些，主要包括：

- 通过文本短信和多媒体短信传播

病毒可以通过影响智能电话的文本传输能力和 PIM 数据，将病毒传播到其它手机上。在支持 MMS 文本功能的手机上，Mabir 病毒就可以通过回复短信实现传播。在西班牙，Commwarrior 病毒可以将病毒发送到手机中的联系人的手机上。

- 蓝牙

蓝牙设备在处于“可发现”模式时会给窃听者提供敏感信息，他们会通过这些信息来访问你的设备。BlueBug 攻击可以让攻击者在被攻击的蓝牙手机上拨打电话、发送和接收短信、阅读和编写电话簿联系人、偷听电话内容以及连接至互联网。BlueDump 攻击通过蓝牙设备的配对信息破解 PIN 码。BlueSmack 攻击通过发送“ping-of-death”消息，可以使蓝牙设备崩溃。BlueStab 攻击利用特殊格式的名字在蓝牙设备自动发现时造成设备崩溃。BlueSnarf 可以让攻击者从蓝牙设备上获取联系人信息和日程数据。

- 播放被精心修改过的多媒体文件

这种攻击方式在固定设备时代就存在，通过诱骗受害人在移动设备上播放被精心修改过的音频或视频文件，造成播放软件甚至系统的崩溃。

- 通过与 PC 机互联

移动设备经常需要与 PC 机互联，进行数据同步。如果 PC 机上安装了恶意程序，它会通过两者间的互联通路入侵到移动设备上，窃取数据。

- 安装未经安全检验的第三方应用程序

有些攻击者在移动应用软件在线市场散布含有恶意代码的应用，或是篡改经过安全认证的应用并在网络上分发。移动设备使用者如果随意从网络上下载应用并安装，很容易感染恶意代码。

欺骗的网络连接是针对移动设备的网络层的威胁。移动设备的网络连接通常是无线链路。攻击者可以设置伪装的无线接入站点，引诱用户设备与伪装的接入站点进行连接，从而监听用户的互联网通

讯或实施钓鱼攻击。通过伪造 GPS 信号对目标设备进行 GPS 欺诈攻击。

### **3、移动设备安全策略与最佳实践**

#### **3.1 物理安全策略**

在机场、图书馆等公共场所中，注意看管好自己的物品，不要让移动设备离开自己的视线。不要将移动设备存放在没有人照看的汽车中，以防被盗。其它一些防盗措施包括：

- 1 记录设备的有关的细节信息：如电话号码、品牌型号、颜色外观、设备 ID 号、GSM 手机的 IMEI 号码、PIN 号码等。
- 2 用记号笔在设备和电池上做上标记。如可以写下住址的单元号码、生日日期等等。
- 3 启用 PIN 或者安全锁密码，锁住移动设备。
- 4 将移动设备的 IMEI 号码在运营商那里进行注册，一旦设备被盗，可以申请运营商阻断被盗设备。这样做的风险是即使找回被盗设备也无法继续使用了。

另外，采取一定技术手段，一旦移动设备被盗，可以顺利定位被盗设备的位置。例如可以在移动设备上安装追踪定位软件，当被盗设备接入互联网，它会悄悄的与公司的监控中心联系，公司可以在权威部门的配合下追踪并收回被盗设备。

#### **3.2 网络安全策略**

在网络接入层对移动设备进行准入认证。安装了指定的客户端安全检查软件的移动设备才准予接入网络。这个策略与固定终端网络环境下的要求是一致的。所不同的是，对于移动设备多数情况下

使用无线链路，为了避免移动设备接入到欺诈网络，对无线设备的准入控制应该是双向的，即符合准入条件的可以接入企业内网，同时也不能随便接入未经认证的网络。这种阻止移动终端接入非认证网络的工作机制同样是依靠客户端软件与认证服务器之间的通讯进行准入判断。

#### **3.3 操作系统及应用程序安全策略**

操作系统的安全策略主要包括三个方面，一是正确进行配置，避免因配置缺陷而遭受攻击。二是避免随意安装未经安全认证的应用程序。三是及时进行系统更新和应用程序的版本升级。为了实现上述目标，应该：

- 在企业内部建立移动设备的应用程序库，程序库中的应用程序都是经验过安全验证，证实没有安全问题的。移动设备只能从应用程序库中下载安装程序；
- 为移动设备提供转译服务，避免在移动设备的本地打开附件；
- 此外还应对移动设备的配置定期进行渗透测试和配置核查，及时发现移动设备上的各种脆弱性。

#### **3.4 数据安全策略**

数据安全策略的目的是防止传输中的数据泄露。这些策略包括数据存储和清除以及通信数据的加密两个方面：

- 企业应该明确规定机密数据范围以及可存放于移动设备的数据的范围；
- 要求机密数据必须存储于加密空间；
- 支持远程删除丢失或遭窃设备中的数据；

- 对重要业务系统的访问需要通过加密通道;

- 从公网访问企业内网, 必须通过 VPN 链路。

### 3.5 安全管理策略与实践

在固定终端设备中的一些安全管理要求, 同样适用于对移动设备的管理。例如对密码口令设置的要求(口令的强度要求以及更换周期等)。

应该以书面形式将前述的各个层面的安全策略以正式的文档公布出来, 并要求使用移动设备的员工签订安全责任书, 以正式明确相关义务。

落实执行前述安全策略, 需要有一套 IT 支撑系统, 从技术上保证对移动设备的统一监控和管理。通常这个系统称为移动设备管理(MDM, Mobile Device Management)系统。下一节将简述 MDM 系统应具备的主要功能。

### 4、MDM 系统的核心功能要求

MDM 系统已经成为国际公认的新的产品门类, 这个领域里的厂商也接近 10 家,

各家的产品功能在细节上虽有差异, 但公认的核心功能包括:

- 设备跟踪定位

移动设备丢失后, 监控中心可以根据监控到的信息, 追踪到设备的实际位置。

- 声音告警及归还信息提示

设备如果丢失, 能发出告警声音震慑盗窃者。同时提供联络方式, 以便捡拾移动设备是人可以根据地址归还设备。

- 网络准入控制

提供双重网络准入控制, 未经认证无法接入办公网, 同时不能接入到不可信任的网络。

- 提供可信的应用程序下载以及附件转译服务

为移动设备提供可信软件下载和邮件转译服务, 避免在移动设备的本地打开附件。

- 远程数据删除

远程删除丢失或遭窃设备中的数据, 通过门户、移动 web 门户或来自好友设备的短信即可实现。支持对移动设备和 SD 卡的全部数据的远程管理。

- 数据加密存储、集中备份和自动恢复

将公司指定的机密数据和个人信息数据存放于加密空间。

- 应用日志

对通话、短信、彩信、网络浏览等活动记录下日志并进行审计, 以便发现滥用行为。

- 集中监控和用户自服务门户

可以让用户通过门户和简单的设备界面快速执行所需的安全任务、备份、定位、擦除等功能。

### 5、结束语

随着云计算和无线宽带数据通信的推广普及, 移动设备的发展会呈现四大趋势, 一个保有数量会加速增长; 二是移动终端会逐步取代传统的固定终端; 三是智能手机会与现有的平板电脑融合成一个综合性的多功能个人移动信息终端; 四是多功能个人信息终端的操作系统在市场大潮的冲刷淘汰下, 剩下 2-3 种主流的系统。

在这种的大发展趋势下, 移动信息终端的安全问题还会层出不穷, 针对个人信息终端的安全管理将成为企业 IT 运维人员重点关注的问题。移动设备管理系统已经成为一个专门的安全产品门类。

# 浅谈下一代防火墙的现状与未来

产品管理中心 段继平

**摘要：**近年来，下一代防火墙（简称 NGFW）作为最具热点的安全产品之一，已经越来越受到国内外安全厂商、市场研究机构、媒体以及 IT 管理者等的追捧。为了帮助大家更好的理解下一代防火墙，本文以安全需求作为出发点，从产品定义与 UTM 等同类产品的区分、未来发展趋势等多个维度，对下一代防火墙做一个全面的剖析。

**关键词：**下一代防火墙 NGFW UTM 硬件防火墙 应用可视 虚拟化安全

防火墙作为网络安全的基础设施，已经拥有 20 多年的历史。从早期的基于 ACL 列表的软件防火墙，到今天应用广泛的基于状态包过滤的纯硬件防火墙，防火墙已经成为信息安全领域中最成熟的产品。

然而，随着攻击技术的不断进化以及云计算、Web2.0 技术等新技术的不断发展和应用，传统的防火墙已经越来越无法满足现在的安全需求，具体表现在以下几个方面：

1. 面向服务的架构及 Web2.0 的广泛应用，大量应用建立在 HTTP 等基础协议之上，而基于端口及 IP 的机制传统防火墙，无法有效识别和管理这些应用；

2. 越来越多的新型安全威胁如社交网络蠕虫、僵尸网络等传播渠道变得越来越隐蔽，传统防火墙无法有效发现和阻止这些威胁；

3. 传统防火墙基于 IP 地址的用户识别及管理的机制，已经变得越来越复杂且难以管理；

4. 随着网络带宽的迅速增长，主流网络带宽已经从千兆时代进入到万兆甚至十万兆时代，传统防火墙无法提供足够的性能和扩展性来应对这种变化。

面对如此复杂的安全需求，作为传统防火墙替代品的 UTM（统一威胁管理）虽然解决了安全功能集成化的问题，但是由于其安全功能未能充分融合以及被人诟病的性能问题，使得 UTM 在这些安全需求面前显得捉襟见肘。而 IPS 产品由于其功能相对单一，显然只能作为传统防火墙的补充方案，而无法真正替代传统防火墙。

在这个背景下，下一代防火墙应运而生

了。那么何为下一代防火墙呢，下一代防火墙与传统防火墙、UTM、IPS 等有什么不同，下一代防火墙未来将走向哪里？我们尝试在下面的章节中找出答案。

## 一、下一代防火墙定义

国际著名的咨询机构 Gartner 认为，下一代防火墙至少应具备以下特征：

- 线速的处理性能

下一代防火墙需要在不影响网络运行的情况下进行嵌入式配置。也就是说，下一代防火墙需要具备线速的网络处理性能，从而实现无缝的部署至现有的用户网络中。

- 高度融合 IPS 能力

所谓高度融合 IPS 能力，并不是简单的将 IPS 功能模块加入到下一代防火墙产品中去，而是要通过一体化引擎，一体化安全策

略框架等技术实现 IPS 策略与传统安全策略的融合，从而最大化的保证系统运行效率。

• 应用可视与身份鉴别的能力

下一代防火墙要具备极强的应用可视能力，用户身份鉴别能力，以及将应用识别及身份鉴别与安全策略整合的能力，这样才真正做到辨别“谁在什么地方访问了什么应用”。

• 传统防火墙功能

既然是要替代传统的防火墙产品，那么下一代防火墙应当具备传统状态监测防火墙所应当具备的全部功能，其中包括包过滤、NAT、状态监测、VPN 等功能。

**二、区分下一代防火墙与 UTM**

为了帮助大家更好的区分下一代防火墙与 UTM 的异同点，笔者从产品架构、应用场景、技术及市场趋势三个方面来对它们进行区分。

• 产品架构

目前主流的 UTM 产品由于在单一设备上集成了大多数安全功能，导致性能成为一个主要瓶颈。主要原因是 UTM 仅仅是把多种安全引擎叠加在一起，而不是从底层进行重新架构设计，这样做的结果就是数据流会在每个安全引擎分别执行解码、状态复原等操作，从而导致大量消耗系统资源，所以当 UTM 启动全部功能时，系统性能大幅度降低也不足为奇了。

而下一代防火墙在设计之初便意识到了这种问题，普遍采用一体化引擎的软件架构。这种一体化引擎架构可以保证在数据流经过系统时，一次性的完成策略查找，应用程序识别 / 解码以及内容扫描

(病毒、间谍程序、入侵防御)等工作，同时结合先进的硬件平台，从而实现最高的处理性能及最小的延迟。

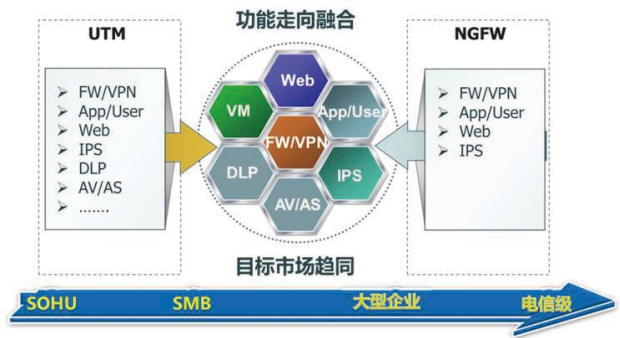
• 应用场景

UTM 集成了防火墙、VPN、IPS、防病毒、防垃圾邮件、广域网加速、上网行为管理等众多安全功能，具备安全功能全面，管理成本较低的优点，同时由于其开启多种功能特性后系统性能急剧下降的问题，因此 UTM 更适合于对产品性价比比较敏感的中小企业用户使用。

而相对于 UTM，下一代防火墙更具优势，下一代防火墙在强调功能融合的同时，又强调一体化引擎的理念，从而保证了开启全部功能后性能仍然保持较高水平，因此下一代防火墙更适合运用于对性能要求苛刻的大型企业和机构的网络。

• 技术及市场趋势

不可否认，无论下一代防火墙还是 UTM，它们共同体现的产品趋势为安全功能高度集成化，即将多种安全功能高效集成至高性能安全硬件中，实现在网关处对安全威胁的综合防御的效果。因此无





论从功能上还是市场定位上,下一代防火墙与 UTM 最终将逐渐趋同,最终的结果便是彼此功能走向融合,市场也逐步统一。

### 三、下一代防火墙的技术发展趋势

随着云计算大潮的袭来,国内云计算与虚拟化技术已经由单纯的理论研究逐步走向实践,新的虚拟化和云计算产品将被更多的企业用户所采用,各种网络应用模式及架构将越来越复杂。因此,对于下一代防火墙来说,将来面临更多新的安全需求,主要体现在:

- 虚拟化安全成为一个亟待解决的问题

随着虚拟化技术的不断发展,以及新一代数据中心的逐渐转型,必然要求下一代防火墙需要具备虚拟化防护的能力,比如如何让防火墙能够与服务器虚拟层沟通,进而能够针对每一台虚拟机的流量做扫描与阻挡,而不会将之视为单一的实体服务器;如何让其硬件资源,能够依照不同功能负载量的状况动态分配,从而能够满足云端的需求等等。

- 新应用模式下的攻击手段及技术将更加复杂及隐蔽

面对不断出现的新的攻击方式及漏洞情况,下一代防火墙需要持续且快速的更新其攻击特征库及不断改进对攻击的防范能力。

- 基于云安全模式的 Web 信誉评级将成为新的需求热点

随着云计算应用的不断普及,用户在享受互联网便利服务的同时,也将受到大量诸如虚假信息、欺诈行为、垃圾邮件、钓鱼网站、恶意代码网站等威胁。因此下一代防火墙需要对互联网资源(域名、IP 地址、URL 等)进行威胁分析和信誉评级,将含有恶意代码的网站列入 Web 信誉库,以阻止对挂马网站的访问请求,实现对终端用

户的安全保护。

- 大量数据中心的新建及扩容将会带来巨大的成本压力

新一代数据中心的建设必然会涉及到网络的不断升级扩容及资源的不断增加,而购买了传统防火墙产品以后,软硬件无法进行对应的升级及扩充,这样必然会导致资源的大量浪费及用户采购成本的大量增加,而下一代防火墙需要更加弹性的软硬件架构来降低用户的采购及升级换代成本。

总之,纵观网络安全的发展史我们发现,任何一次 IT 信息技术的变革,必然会给安全产品带来新的需求及产品方向。下一代防火墙诞生的时候正是处于云计算、WEB2.0 等 IT 新技术革新的时代,我们有理由相信,只要能够准确把握用户需求,不断的进行技术创新,下一代防火墙必然能够在未来走得更远。

### 四、结束语

任何一个新的产品从诞生到成熟必然会经历一个过程,同样下一代防火墙作为一个革新性的产品也将会面临技术和市场等多方面的挑战。

从技术角度来看,下一代防火墙强调一体化引擎和安全功能融合的技术理念无疑是领先的,然而领先的技术理念能否转化为具有核心竞争力产品从而真正满足用户的安全需求,还需要接受时间的检验。

从市场的角度来看,下一代防火墙定位于传统防火墙、UTM、IPS 等网类产品替代者,在其进入市场后必然会受到后者的前后夹击,如何找准自己的定位,并且在传统网关市场这一红海中成功杀出重围,将会是下一代防火墙将要面临的首要问题。

# 浅谈蜜网在电信运营商行业中的应用

行业营销中心 唐洪玉

**摘要：**本文对蜜罐及蜜网进行了介绍，对蜜网的数据控制、数据捕获、数据分析的核心功能进行了阐述，并对蜜网在运营商的应用进行了探讨和分析，讲述如何利用蜜网技术来帮助运营商完善现有的防御体系，增强安全防御的积极性和主动性。

**关键词：**蜜罐技术 蜜网技术 安全威胁 电信运营商

## 一、前言

随着网络攻击技术的发展，特别是分布式拒绝服务攻击、跳板(Step-stone)攻击及互联网蠕虫的盛行，互联网上的每一台主机都已经成为攻击的目标；而且，特别值得注意的一个趋势是多种攻击脚本和工具的融合，如大量的内核后门工具包(Rootkit)、能够集成多种攻击脚本并提供易用接口的攻击框架的出现，使得攻击“无处不在”，简单易行。

同时，电信运营商网络的建设规模在不断扩大，其所面临的安全威胁也在急剧增加，安全风险不断被放大。然而，当网络系统被攻击后，对于对手是谁、他们使用了哪些工

具、以何种方式抵达攻击目标等，运营商对这些都一无所知。

面对日益复杂的入侵事件，运营商目前所广泛采用的传统的被动防御手段已很难满足当前的需求，因此必须采用一种新的技术手段，增强安全防御工作的积极性和主动性，而这种技术的首选就是蜜网。

## 二、蜜网技术简介

### 2.1 蜜网的基本概念

蜜罐(Honeytrap)，简单来说，是一项技术、一种安全资源，它的价值就在于被探测、攻击和破坏。蜜网(Honeynet)，是在蜜罐(Honeytrap)技术上逐步发展起来的一个新的概念，它实际上是一种研究型的、

高交互型的蜜罐技术，其主要目的是收集黑客的攻击信息。与传统蜜罐技术的差异在于，蜜网构成了一个黑客诱捕网络体系架构，在这个体系中包括：

- 一个或多个蜜罐
- 多层次的数据控制机制
- 全面的数据捕获机制
- 深入的数据分析机制

### 2.2 蜜网体系框架

如图1所示，一个典型蜜网体系框架由蜜罐主机、蜜网网关和日志服务器/监控管理平台等三部分构成。其中，蜜网是与内部业务网络并行的网络，由多个蜜罐主机组成；所有进出蜜网的流量都需要经过蜜网网关；日志

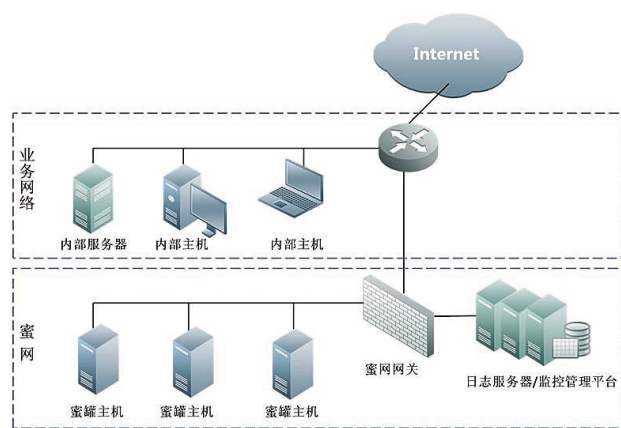


图 1 典型蜜网体系框架图

服务器（监控管理平台）对蜜罐主机及蜜网网络产生的日志数据进行收集，提供后续分析。

蜜网有三大核心需求：数据控制、数据捕获和数据分析。通过数据控制能够确保黑客不能利用蜜网危害第三方网络的安全，以减轻蜜网架设的风险；数据捕获技术能够检测并审计黑客攻击的所有行为数据；而数据分析技术则帮助安全研究人员从捕获的数据中分析出黑客的具体活动、使用工具及其意图。

### 2.2.1 数据控制功能

数据控制的目的是阻止攻击者在获得蜜罐的根权限后，利用蜜罐作为跳板向外发送非法信息或者攻击其它机器。

数据控制功能，由蜜网网关完成。蜜网网关对流入蜜网的数据包不做限制（或依据需要对部分数据进行过滤或限制），使得黑客能攻入蜜网；但对黑客使用蜜网对外发起的跳板攻击进行严格控制。

控制的方法包括攻击包抑制和对外连接数限制两种手段：

1) 攻击包抑制，主要针对使用少量连接即能奏效的已知攻击（如权限提升攻击等）。例如使用基于规则的攻击包抑制器，检测出从蜜网向外发出的含有的攻击特征的攻击数据包，发出报警信息并对攻击数据包加以抛弃或修改，使其不能对第三方网络构成危害。

2) 对外连接数限制，主要针对网络探测和拒绝服务攻击。蜜网网关通过在内置防火墙中设置规则，当黑客发起的连接数超过预先设置的阈值，则内置将其记录到日志，并阻断其后继连接，从而避免蜜网中被攻陷的蜜罐作为黑客的跳板对第三方网络进行探测或拒绝服务攻击。

### 2.2.2 数据捕获功能

数据捕获的目标，是捕捉攻击者从扫描、探测、攻击，到攻陷蜜罐主机，最后离开蜜罐的每一步动作。

数据捕获功能，由蜜网网关和安装在蜜罐主机上的主机行为监视模块共同完成。

蜜网网关内置网络攻击检测模块，对流入蜜网的数据包基于规则进行告警，产生告警日志，同时捕获原始流量数据包，生成 netflow 流数据。在各蜜罐主机，安装可自我隐藏的主机行为监视模块，对蜜罐主机的各种变化情况，如进程变化、网络连接变化、文件变化、注册表变化……进行记录，生成日志，并且捕获样本文件，以隐藏协议栈传输的方式传到蜜网网关，再传到日志服务器（监控管理平台）。

### 2.2.3 数据分析功能

数据分析，是要从大量的网络数据中提取出攻击行为的特征和模型，通过数据融合和关联分析，了解和掌握攻击者所用的技术、动机、新工具和新方法。

### 2.3 蜜网的优势

蜜网技术，在捕获和了解 Internet 安全威胁方面，具有以下优势：

1) 在蜜网环境中没有任何业务网络流量，所有蜜网捕获的网络流量都可以认为是恶意的，使得蜜网捕获网络流量相对较少；

2) 蜜网环境中不依赖于任何区分正常流量和恶意流量的检测分类算法，保证了蜜网环境极低的误报率，同时也使其具备对未知安全威胁的捕获和发现能力；

3) 蜜网环境提供了完善的数据控制和数据捕获能力，能够帮助安全分析人员减少安全威胁带来的安全风险，同时能够给出对攻击场景全面且深入的观察数据。

### 三、蜜网在电信运营商行业的应用探讨

运营商目前所采取的安全防护手段，从网络安全防御思想来看是一种被动的网络防御手段，主要还是基于已知攻击的特征来进行安全防护，可以较好地解决已知的网络安

全威胁问题，但是对于未知攻击还是无能为力。

蜜网作为一种主动技术，将改变传统防御手段的被动处境，使其具有攻击捕获和智能分析的反应能力，弥补传统网络安全防护体系的不足。

#### 3.1 行业应用探讨

蜜网技术在运营商网络安全方面的应用，会给运营商带来保障网络与信息安全的新能力，主要表现在以下几个方面：

##### 1. 定位识别攻击者，为安全运维提供有力支撑

利用蜜网技术，可以有有效的监测和定位攻击者，特别是位于内网的攻击者。根据攻击者对内容的兴趣方向、采取的操作，分析其身份目的，通过跟踪功能对入侵者进行有效的追踪，并配合入侵取证功能对黑客入侵行为进行法律取证及有力的打击。

同时，对攻击进行有效定位和识别后，将相关数据提供给安全运维系统，使运维人员可以更好的应对网络攻击，提高安全运维的响应速度和质量。

##### 2. 网络安全状况监控，了解安全威胁状况

蜜网的应用和部署，可以捕获到各种攻

击，如恶意代码（病毒、僵尸、蠕虫）、自动化攻击工具攻击、扫描探索式攻击、未知攻击等等。同时，借助蜜网强大的数据分析能力，将有助于运营商安全运维人员对当前网络状况的跟踪分析，及时了解系统可能面临的安全威胁。

##### 3. 进行攻防演练培训，提高培训质量

网络安全攻防演练培训，是提高运营商安全运维人员实战能力的重要途径。利用蜜网技术搭建攻防演练平台，通过虚拟蜜网技术可以模拟各种网络服务及系统漏洞；通过数据控制能够确保攻防演练的行为可控，保证演练平台的安全性；数据捕获技术能够检测并审计攻防演练的所有行为数据；而数据分析技术则帮助教师和学员从捕获的数据中分析出攻击方的具体活动、使用工具及其意图，增强实战技能。

##### 4. 进行业务应用系统软件的安全性测试

利用蜜网技术，搭建业务应用软件的网络安全性能测试平台，对该业务应用系统进行模拟和实战攻击，将可以有有效的降低应用系统软件存在的技术漏洞等安全隐患，为应用系统的安全性测评提供数据支持。

##### 5. 监测定位僵尸主机

## ▶▶ 行业热点

通过部署蜜网，搜集恶意软件，对其样本进行分析，确认是否僵尸程序，并对僵尸程序所要连接的僵尸网络控制信道的信息进行提取，最后通过客户端蜜罐技术，伪装成被控制的僵尸工具，进入僵尸网络进行观察和跟踪，进而发现整个僵尸网络的构成，进行 Botnet 主机的定位。

### 3.2 应用案例分析

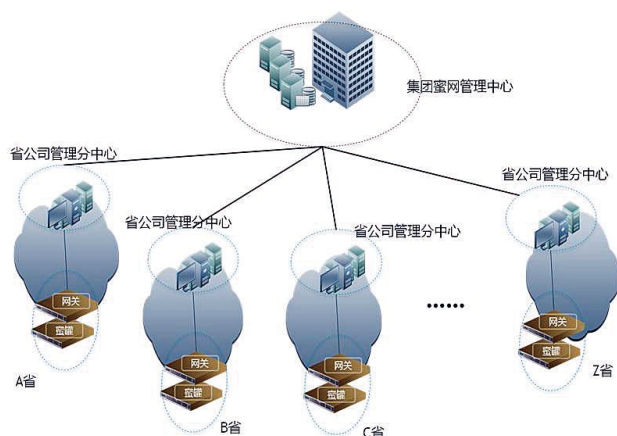


图2 运营商全国蜜网部署图

如图2所示，在运营商的IP网上，进行全国蜜网的分级部署：集团部署全国蜜网管理中心，各省公司部署管理分中心和蜜网网关、蜜罐系统。这样，对全国捕获到的攻击统一进行分析和处理，从而获得整体的安全威胁状况。同时，每个省的管理分中心可以对本省的蜜网系统进行管理和数据的分析。

接下来，本文将通过一个发现、分析、封堵 Botnet 的例子，来

对蜜网在运营商安全运维工作中的具体应用进行分析和阐述。

#### 1.Yoyoddos 的发现和捕获

如图3所示，通过蜜网系统，捕获到 Yoyoddos.exe，经过蜜网内置的多种扫描引擎确认，发现是恶意的后门软件。从图3中，还可以看出，对于 Yoyoddos 的捕获已经多达 409 次，且在多省被捕获。

样本消息/捕获情况					
样本消息信息		引擎识别信息		本月捕获次数	累计捕获次数
最早捕获时间	md5 HASH			0	409
08:50:04	2060dfc06baee76b566b3f437338fbc3	Backdoor.Win32.PoisonIy.In.加亮(UPX),卡巴斯斯基(3/4)			
样本捕获信息(最近10条)					
捕获日期	捕获蜜罐	原始文件名	进程ID	捕获蜜罐配置信息	
04:58:20	江苏 /Win 300Server	yoyoddos.exe	1544	操作系统:(Windows2000Server,Windows,高交互蜜罐);服务状态:	
04:58:12	江苏 /Win 300Server	boot1.exe	1004	操作系统:(Windows2000Server,Windows,高交互蜜罐);服务状态:	
04:35:18	山西 indows2003	yoyoddos.exe	1800	操作系统:(Windows2003,Windows,高交互蜜罐);服务状态:	
04:35:17	山西 indows2003	boot1.exe	432	操作系统:(Windows2003,Windows,高交互蜜罐);服务状态:	
04:34:50	河南 indowsXPsp0	yoyoddos.exe	296	操作系统:(WindowsXPsp0,Windows,高交互蜜罐);服务状态:	
04:34:44	河南 indowsXPsp0	boot1.exe	1448	操作系统:(WindowsXPsp0,Windows,高交互蜜罐);服务状态:	
04:24:41	山西 indowsXPsp0	yoyoddos.exe	328	操作系统:(WindowsXPsp0,Windows,高交互蜜罐);服务状态:	

图3 Yoyoddos 捕获情况

#### 2.Yoyoddos 的特征及攻击行为分析

如图4所示，蜜网系统可以捕获并显示被感染主机的进程和文件的变化，这可以帮助我们了解 Yoyoddos 的感染过程和行为进行了了解和分析。同时，利用蜜网系统，也可以对其攻击场景进行还原。

通过分析，发现当一台主机被这种木马感染后，会生成 %SystemRoot%\system32\yoyoddos.exe 文件，并生成注册表键 HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\yoyoddos，将 Yoyoddos.exe 注册为 Windows 自启动服务。Yoyoddos 服务运

行后会连接远端服务器，加入 yoyoddos 僵尸网络，听取并执行攻击命令。

进程ID	PPID	结束进程的进程ID	用户PID
1820	1544	1820	0
1544	864	1544	0
564	1544	564	0
1820	1544	1544	0
1544	864		0

进程ID	PPID	结束进程的进程ID	用户PID
1820	1544	1820	0
1544	864		0

图 4 被感染主机进程和文件变化状况

```

15:09:49, COMMAND="TCP-FLOOD(3)", Target="222.222.160:2551"
ThreadCount=40.
15:10:07, COMMAND="STOP_FLOOD(14)".
15:10:39, COMMAND="TCP-FLOOD(3)", Target="222.222.161:2551"
ThreadCount=40.
15:10:42, COMMAND="STOP_FLOOD(14)".
15:10:55, COMMAND="TCP-FLOOD(3)", Target="222.222.160:2551"
ThreadCount=40.
15:11:01, COMMAND="STOP_FLOOD(14)".
15:18:56, COMMAND="DOWNLOAD-AND-EXEC(15)",
URL="http://123.123.8080/dos.exe".
15:22:28, Parse C&C URL "qq333333.org" to "123.123.102",
Port=2009.
15:22:29, Connect to "qq333333.org 2009".
15:44:07, Parse C&C URL "qq333333.org" to "123.123.102",
Port=2009.
15:44:07, Connect to "qq333333.org 2009".
15:46:54, COMMAND="UDP-FLOOD(2)", Target="174.174.168:80",
ThreadCount=8.
15:47:46, COMMAND="STOP_FLOOD(14)".
    
```

图 5 Yoyoddos 行为分析

对 Yoyoddos 进一步的跟踪分析，得出如图 5 所示的信息，从中可以发现 Yoyoddos 的攻击行为，包括具体的 botnet 指令，如 TCP FLOOD、UDP FLOOD 等。

在图 5 中，可以看出，僵尸主机和远端控制服务器“qq\*\*\*.org”（123.\*\*.102）取得联系，进行通信，听取指令。同时，可以看出，该僵尸网络曾先后对“222.\*\*.160”、“222.\*\*.161”进行了 TCP FLOOD 攻击，并分发了新样本“http://123.\*\*.8080/dos.exe”。

### 3.Yoyoddos 的封堵

从上述分析可以得出，该感染主机的远程控制端是“qq\*\*\*.org”（123.\*\*.102），并接受指令对外进行了 DDoS 攻击。那么，如何对该 Yoyodos 僵尸网络进行封堵和治理呢？

首先，在 IP 网相应的网络设备、DNS 服务器、安全设备上对远程控制端的 IP 地址和域名进行封堵和禁止访问；同时，通过监听网络内和该控制端发生的通信，进一步定位网内的其他 Yoyoddos 主机，给予全面的打击和遏制，使这种 Yoyoddos 在该运营商的 IP 网中不再泛滥。

### 四、总结

蜜网技术的出现，使得我们可以变被动防御为主动进攻，使其具有主动交互性。通过蜜网在电信运营商行业中的应用和部署，可以使运营商主动了解入侵者的思路、工具、目的和机制，发现潜在的安全威胁，并且针对这些威胁及时找出相应的防御策略，以此来提高系统的安全性。可见，蜜网的应用，对保障运营商的网络安全有着非常重要的意义。

# 金融机构反钓鱼监控体系建设方案

行业营销中心 陈星霖

**摘要：**钓鱼攻击引发的安全事件，涉及到国内多家商业银行，已经严重损害了投资者的利益，影响了金融机构的声誉，以及整个金融市场的稳健发展。金融机构有必要建立一个完善的反钓鱼监控体系，以提高网上银行系统的风险防御能力。在技术内刊总第13期上，笔者介绍了钓鱼攻击的研究和对策，这篇文章会给出一种较为可行的思路，即基于钓鱼攻击发生的时间线索，从“事前预警”、“事中防御”和“事后整改”三个阶段，分别实施有针对性的监测和控制。

**关键词：**反钓鱼、反钓鱼技术、反钓鱼网站安全监测系统、网络钓鱼 / 钓鱼攻击、业务风险防控

## 引言

钓鱼攻击引发的安全事件，涉及到国内多家商业银行，已经严重损害了投资者的利益，影响了金融机构的声誉，以及整个金融市场的稳健发展。为了有效应对钓鱼攻击，维护公众利益和企业声誉，金融机构有必要建立一个完善的反钓鱼监控体系，以提高网上银行系统的风险防御能力。

中国银监会于2011年3月15日发布了《关于进一步加强网上银行风险防控工作的通知》，要求各银行业金融机构应高度重视网上银行风险管控，加强对仿冒网站等“钓鱼”

欺诈事件的防范。同时，加强“反钓鱼”应急处置机制建设，有效切断“钓鱼”诈骗渠道。

如何及时、准确地发现钓鱼网站，并予以有效的控制和阻断，已经成为金融机构亟待解决的问题。该文档给出的“反钓鱼”监控体系建设思路和建议，希望能给大家带来一些启示。

## 一、基于“事前-事中-事后”循序改进的反钓鱼监控思路

建设一个积极、主动的“反钓鱼”监控体系，一方面需要依托互联网环境的监管和治理；另一方面应该坚持贯彻“预防为主，

防治结合”的方针，深入挖掘金融机构可能被钓鱼攻击利用的各种潜在威胁，主动找寻、实时监测互联网上网络钓鱼相关的安全风险，多方面积极控制钓鱼攻击可能带来的影响，为网上银行风险防控工作提供先进的技术支撑，为金融机构业务拓展提供强有力的安全保障。

那么，究竟应该如何建立“反钓鱼”监控体系，同时确保这个体系的有效性和完整性呢？一种较为行之有效的思路是：基于钓鱼攻击发生的时间线索，从“事前预警”、“事中防御”和“事后整改”三个阶段，分别实

施有针对性的监测和控制。

#### • 事前预警

在钓鱼网站真正产生危害之前，即便钓鱼网站已经存活，但没有发现，这个阶段都可定义为“事前阶段”，主要解决如何及时发现钓鱼网站，并通知用户的问题。在这个阶段，可结合定期主动评估、实时安全监测等技术手段，及时找到可能被钓鱼攻击利用的弱点，第一时间协助金融机构启动紧急预案，做出响应。

#### • 事中防御

从发现钓鱼网站开始，到关闭这个恶意站点，整个阶段定义为“事中阶段”，包含至少一次完整的钓鱼攻击，那么这个阶段主要考虑如何控制钓鱼攻击的影响。在发现钓鱼网站之后，往往采用多种方式控制钓鱼攻击可能带来的影响，主要包括关停域名、阻断终端用户对钓鱼网站的访问等方法。

#### • 事后整改

针对钓鱼攻击的后续处理阶段，可统称为“事后阶段”。处置完钓鱼网站之后，在案例总结分析的基础上，需要及时修补被钓鱼攻击利用的弱点，并进一步加强终端用户培训和教育，以减少同类事件的发生概率。

有了明确的时间边界，以及确定的防护需求和工作目标，反钓鱼解决方案才能更充分、更完整地发挥其应有的效益。基于此思路，循序改进，从而最终建立一个完善的反钓鱼体系。

## 二、事前预警的主要技术手段

对抗网络钓鱼以预防为主，如果能及时昭示钓鱼风险的前兆，

超前反馈，快速布置，则在一定程度能够有效防范钓鱼事件的发生，在信息安全对抗过程中，也能处于更加积极、主动的位置。

事前预警阶段，需要在钓鱼者之前，尽可能多地找出各种可能被钓鱼攻击利用的弱点，包括来自业务系统自身的缺陷，业务系统运行的支撑环境弱点，以及来自互联网的安全威胁。所以，本阶段可以考虑综合使用业务安全风险评估、业务环境脆弱性评估，以及钓鱼风险实时监测等多种方法，以确保预警工作的完备性。

### 2.1 业务安全风险评估

业务流程的设计失误同样会引入网络钓鱼等各类风险，如网银系统虽然采用了双重用户身份认证手段，但如果没有考虑登陆和交易两类业务单元的逻辑顺序以及相互依赖性，钓鱼者利用窃取到的用户账号、密码对，就能够即时完成登录和转账等操作，直接导致用户个人财产损失。所以，及时找出业务流程中存在的问题，既有助于保障业务系统的正常运转，又能防范钓鱼攻击等安全事件的发生。

业务安全风险评估，是一种基于安全目标的业务流程分析方法，从目标业务系统的关键流程步骤分解入手，分析每个步骤具有的安

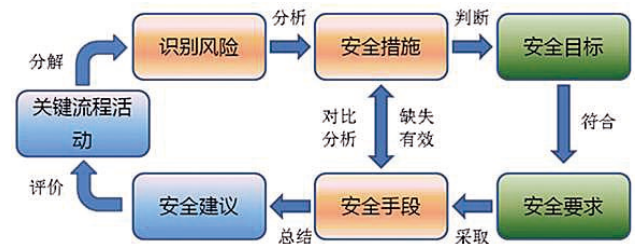


图 1 基于安全目标的流程分析方法



全风险，及防范风险所采取的安全措施，判断各项功能的安全措施是否符合为实现安全目标所要达到的安全要求。同时，对业内达到该安全要求普遍采取的安全手段与现有安全措施进行对比分析，主要关注两个方面：安全措施是否有缺失、安全措施是否有效，最终提出对现有流程的安全建议，对流程进行客观评价。

采用业务流程安全风险评估的方法，可以让金融机构清楚地识别出业务流程每一个关键步骤可能面临的风险，在对业务目标，以及现有安全控制措施做出客观评价之后，最终形成安全现状报告，使金融机构更加清晰地认识到网上银行的整体安全状况，能够给下一步流程整改和优化，带来融合业界最佳实践的指导意见。

## 2.2 业务环境脆弱性评估

钓鱼攻击的一种常见方式，是首先利用网站自身的弱点，或是业务系统运行环境（包括承载业务系统的平台、操作系统，以及相关应用系统等）存在的缺陷，进行渗透，然后再发起钓鱼欺诈。如果能解决上述安全问题，一方面可以保护金融机构的网站不被攻击，另外一方面，也能在一定程度上降低钓鱼攻击发生的几率。

无论是网站的 XSS、SQL 注入漏洞，还是引自第三方内容的数据隐患，以及客户端环境的技术弱点，都可以通过安全技术评估来提前发现。一种传统的思路，是使用漏洞扫描软件进行弱点检查，但需要兼顾评估能力和资源等方面的因素。

一种革新的思路：基于互联网，采用来自“云端”的远程漏洞扫描能力，对网站、业务系统支撑环境进行脆弱性评估。这是一种定制化的，基于“云”的安全服务模式，可结合安全专家的分析，对

网站结构与漏洞、操作系统漏洞，以及域名解析服务器的漏洞，进行定期检查，用户无需采购任何安全漏洞扫描产品，即可获得网站全方位的钓鱼攻击风险评估报告，以及获得修补建议。

因为金融机构的网站、业务系统自身处于持续改进的状态，所以针对业务环境的脆弱性评估工作应该固化下来，定期进行，并予以阶段性的调整和完善。

## 2.3 基于“云”的钓鱼风险实时检测

因为有了确定的防护对象、可控的防护范围，针对业务流程，以及业务环境的安全评估可以定期展开，以确保及时发现金融机构内部信息系统的弱点。而另一类来自互联网，和钓鱼攻击相关的安全威胁，因为存在大量的不确定性，所以一直难以被识别和穷尽。

钓鱼者可能在全球任何一个有 Internet 接入的角落发起钓鱼攻击，这类攻击有着明确的目标，欺骗性很强，会综合利用多种攻击手段，并借助多种渠道传播和实施。钓鱼网站的平均存活时间很短，一般还会选择境外注册和托管，导致国内监管机构难以发挥其应有的效力。如何主动找到互联网上更多和金融机构相关的钓鱼网站，如何长期建立和维护一个有效的恶意钓鱼站点库，已经成为一个极大挑战。

区别于传统被动防范钓鱼网站的发现方式，当前出现了一些更有效的检测与发现方式，“反钓鱼网站监控”服务就是其中一种新型的应用模式。“反钓鱼网站监控”服务是一项基于“云”的一站式托管式服务，承载于专有的“互联网安全监测平台”，主要根据网站所有者的域名、IP 和关键字组合清单，定期对不同传播方式（如搜索引擎）

的相关内容进行监测，监测使用这些信息渠道的访问者被钓鱼攻击的风险。同时，通过对互联网站点进行自动分析，“互联网安全监测平台”能够发现与目标站点相类似的可疑钓鱼站点，在半自动确认后进行报警。

对于钓鱼网站的检测，还考虑采用基于生命周期的检测方式。在访问网站前，对网站的域名、IP 地址进行查询分析，若发现与预设规则不符则判定为可疑网站。这些预设规则往往如域名的使用时间、生效时长、IP 地址与域名的绑定时长等等。

对于使用“反钓鱼网站监控”服务的金融机构，只需要将被监控网站的域名、IP 和关键字组合告知监测中心，即可坐享 7×24 小时的“反钓鱼风险监控”专项支持，相关服务的一般流程示意如图 2 所示。

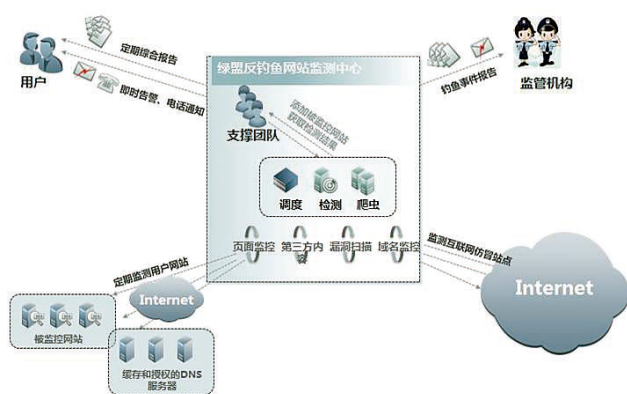


图 2 反钓鱼网站监控服务流程

基于互联网的钓鱼风险实时监测，可以协同业务安全风险评估、业务环境脆弱性评估等方法，形成一套较为完整的预警方案，金融机构应该综合运用上述方法，主动防范可能发生的钓鱼攻击。

### 三、事中主动防御的控制措施

对抗网络钓鱼的方法很多，最有效的方法是同时把几种技术手段和服务结合在一起，以便尽快减缓钓鱼攻击带来的影响。无论是采用自有资源，还是选用外包服务，对抗网络钓鱼都是一个持续需要专家建议的过程。

反钓鱼整体解决方案的事中防御阶段，要综合考虑多方面的因素，既包括在线未经授权交易的及时发现和处理，还包括对非法钓鱼网站的分析、调查、取证，甚至是反制。在本方案中，主要考虑如何整合各种资源，抑制钓鱼攻击影响的问题。

#### 3.1 关停钓鱼网站，切断万恶之源

控制钓鱼攻击，最有效方法的就是直接关停钓鱼网站，从根本上杜绝钓鱼攻击的发生。例如 APAC 在处理这一类问题时，主要通过协调中国互联网信息中心 (CNNIC) 来关停 CN 域名的钓鱼网站。然而随着 CN 域名实名制工作的不断完善，注册 CN 域名制作钓鱼网站将逐渐成为历史，APAC 的统计报告显示，2011 年 6 月，以 CN 域名注册的钓鱼网站仅占处理总量的 0.37%。

关停钓鱼网站还存在一些技术上的难度和局限性。如，境外注册的钓鱼网站，无法快速阻止；钓鱼网站生存周期短，成本低，可快速复制，关停力度凸显不足。另外，停止钓鱼网站的域名解析也有一定风险，如果用户误报了钓鱼网站，一旦被关停将导致法律风险。

为了避免这种风险，在发现可疑钓鱼网站后，必须提交目标机构确认，在获得授权后再上报有关机构，查封恶意域名。

### 3.2 从客户端抓起，及时阻断钓鱼威胁

尽管关停钓鱼网站能够从根本上解决钓鱼问题，但这个过程往往会花费几个小时，甚至几天的时间，这对于分秒必争的反钓鱼工作，是不能接受的。因为难以操作，效力有限（仅针对 .COM 或 .CN 域名生效），金融机构在尝试关停钓鱼网站的同时，还可以同步实施的反钓鱼措施是网站屏蔽，如从客户端阻断可能发生的钓鱼网站访问行为，以减轻钓鱼攻击所造成的损害。

客户端防护仍然沿用传统的，基于黑名单的访问控制策略，在发现终端用户即将访问存在钓鱼风险的页面时，终端系统将弹出一个警示对话框，以揭示当前用户行为的安全隐患。为了避免干扰用户的正常互联网访问行为，终端系统所加载的钓鱼网站黑名单必须是可靠、且能够持续更新的。

结合主动、准确的钓鱼网站检测和发现机制，将最新的钓鱼网站信息，通过客户端提示的方式，快速告知客户，可以很

好地加强最终客户风险防范意识，提高钓鱼网站识别能力，并最终提升安全应对的时效性。

## 四、事后整改和教育

钓鱼攻击的本质问题是人的认知问题，因为无法准确识别出钓鱼网站，才导致终端用户访问了高风险的页面。如果能提升用户对钓鱼风险的识别能力，则能极大降低钓鱼攻击发生的概率。看似普通的安全意识教育，在对抗钓鱼攻击的过程中，反而能产生最大的功效。

反钓鱼整体解决方案的事后整改阶段，一方面要基于当前案例的分析结论，修补业务流程、业务环境存在的弱点；另一方面要加强终端用户的安全意识培训力度，防范于未然。当然，此类培训更应该作为一项日常工作，周期性地持续开展下去。

### 4.1 专项整改行动

顾名思义，专项整改有着明确的目标和改进对象，金融机构可结合定期安全评估的结果，以及在实际钓鱼攻击事件中突显出来的问题，执行针对性的改进措施，包括业务流程优化，可管理的安全服务实施等。

专项整改虽能减小钓鱼攻击再次发生的几率，但不能完全杜绝钓鱼攻击。尤其对于部分短期内无法修补的弱点，如业务逻辑设计缺陷，仍需加强相关方面的日常监测工作。

### 4.2 多样化的安全意识教育

在钓鱼攻击的过程中，人性的弱点暴露无疑，很多受害者都是因为经不起诱惑而落入陷阱。所以严格说来，网络钓鱼并非单纯的技术问题，加强用户对网络钓鱼攻击手法的认识，是解决此类攻击的最好方法。

对于为终端用户提供高质量的金融电子服务的企业来说，金融机构有义务为广大用户普及防钓鱼的相关知识。因此，在网站或相关页面建立专项的“反钓鱼”知识栏目，提供丰富的“钓鱼”案件实例分析，是一种值得应用和推广的方式。为了最大化地吸引用户对知识的学习，可以通过游戏的方式模拟遭遇网络钓鱼的经历，教导用户如何识别可疑站点。

除此之外，教育活动本身应该是形式多样的，可以与终端用户的日常生活、工作结合起来。在加强用户识别可疑站点的同时，增加用户对特定的关键信息进行强化记忆，

可以是特定网站的登录界面、特殊图片、特定信息等，表 1 提到的一些形式和内容，可供参考。

表 1 多样化的教育方式

现场交互类	意识培训	线上的培训材料
	各种交互活动	模拟场景 / 在线问答等
日常提示类	动态 BANNER	在网站或各种服务的登录页面放置安全提示
	张贴标语	在营业厅显眼位置放置张贴画
	警示便签	在电脑、门禁等地方张贴安全提醒便签
	屏幕保护	提供安全意识培养屏保
	易拉宝	安全宣传活动中展现企业安全警讯、口号等
物品提示类	小物品	包含安全提示的各种定制小物件，例如笔筒、钥匙扣之类。
	分发小册子	印刷制作安全小册子，分发客户教育手册。
	电子杂志	专题形式的教育电子杂志

#### 4.3 案例分析和存档

一旦遭遇了钓鱼攻击，金融机构首先应该配合公安机关的调查取证工作，为更快速地挽回客户损失、避免造成影响而努力。同时，还应该主动跟踪钓鱼事件的发展状态，并主动为客户提供法律援助。

最后，应该对事件进行认真的分析总结，形成案例并存档，针对案例提出改进措施和预防建议，以避免类似事件的再次发生。

#### 五、建立多方协作的反钓鱼监控平台

评价反钓鱼体系有效性的两项关键指标是速度和效率，这使得对抗网络钓鱼注定成为耗费时间的资源密集型工作，需要综合应用各种资源，得到多个相关机构的鼎力支持。只有建立一个多方协作的合作平台，集结金融机构、域名注册和管理机构、专业安全公司、IDC，甚至互联网公司等多方优势资源，才能最大限度地发挥反钓鱼体系的作用。

另外，金融机构在遭遇钓鱼攻击等安全事件前，应建立一套清晰的事件处理流程，以确保在遭遇突发事件时，能参照一个规范化、标准化的处理办法，顺利协调到相应资源，并最终及时处理钓鱼攻击。钓鱼攻击的响应流程基本涵括检测、通知和阻断等过程。在一些资源相对充足的反钓鱼体系中，可能会引入多个网络阻塞合作伙伴，包括微软、Google、Cisco 等，以限制钓鱼网站的充分曝光。对于一些研究机构而言，取证和诱捕能够让他们更加清楚地了解到钓鱼攻击的本质，以及具体的攻击手法。这些工作丰富了反钓鱼响应流程的内容，金融机构在建立自己的反钓鱼体系中，需要结合自身需求和资源匹配情况，针对性地进行取舍。

最后，在钓鱼网站防治方面，信息的共享同样重要。建立基于行业的“云”共享平台，是很有必要的，特别是钓鱼网站相关的“云”共享，对于加强检测手段，防范钓鱼攻击都将做出特别贡献。

# 美国《网络空间国际战略》解读

行业营销中心 李文法 孙铁

**摘要：**本文在介绍美国网络空间国际战略相关背景的基础上，分析了美国网络空间国际战略组织结构，对美国网络空间国际战略的重点内容进行了解读。最后，对美国网络空间国际战略进行了总结，并给出了我国建设网络空间的相关建议。

**关键词：**网络空间战略 国际战略 国际战略研究 战略解读

## 一、相关背景

2011年5月16号，美国发布《网络空间国际战略》(International Strategy for Cyberspace)，它是美国国家战略的一部分，是美国网络安全国家战略的延续和进一步深化，这可以从近年来美国网络安全国家战略的发展和演变中得到印证。

### 1.1. 克林顿时代的网络安全主题：基础设施保护

1993年，克林顿政府提出兴建“国家信息基础设施”；1998年，克林顿

发布第63号总统令：《克林顿政府对关键基础设施保护的策略》(The Clinton Administration's Policy on Critical Infrastructure Protection)，成为直至现在在美国政府建设网络空间安全的指导性文件；2000年1月，美国总统克林顿发布《信息系统保护国家计划》(National Plan for Information Systems Protection)，率先提出重要网络信息安全关系到国家战略安全，把重要网络信息安全放在优先发展的位置，并对重点信息网络实行全寿命安全周期管理。按照要求，新建和正在运行的重要信息

网络的信息系统必须实施定期风险评估，针对信息系统的安全类别和等级，实行等级保护，并定期通过安全测试和风险评估，由联邦机构的高级官员基于安全控制的有效性和残余风险值决定是否授权该信息系统投入运行。这些风险评估的方法，逐渐成为全球信息系统安全评估的模式。克林顿时代的网络安全战略重点在于“全面防御”。

### 1.2. 布什时代的网络安全主题：网络反恐

布什上台以后，作为美国重要的核心网站，国防部网站被攻击次数不断增加使美国政府忧心忡忡。9·11事件发生后，一些恐

怖分子利用网络之便向美国计算机网络频繁发动攻击，特别是对要害部门的网络进行破坏，从而危害美国及其盟友国家民众的安全，“网络恐怖主义”浮出水面。

2003年2月，白宫发布《保护网络空间安全国家战略》(The National Strategy to Secure Cyberspace)，该战略勾勒了组织打击由恐怖分子、罪犯或敌对国家发起的网络攻击的工作并确定其重点的初步框架，该战略报告正式将网络安全提升至国家安全的战略高度，从国家战略全局上对网络的正常运行进行谋划，以保证国家和社会生活的安全与稳定。2008年1月，美国总统签署国家安全第54号总统令，国土安全第23号总统令，提出《国家网络安全综合计划》(The Comprehensive National Cybersecurity Initiative)，这是一项多年计划，由多个部门参加并分步骤实施，其最终目的是保护美国的网络安全，防止美国遭受敌对电子攻击，并能对敌方展开在线攻击。

同时，布什非常重视美军网络战进攻能力建设，首先，大力开发计算机网络战武器。在软杀伤网络战武器方面，美军已经研制出2000多种计算机病毒武器，如“蠕虫”程序、“特洛伊木马”程序、“逻辑炸弹”、“陷阱门”等。在硬杀伤网络战武器方面，美国正在发展或已开发出电磁脉冲弹、次声波武器、激光反卫星武器和高功率微波武器，可对别国网络的物理载体进行攻击。其次，创建“黑客部队”。据悉，美军通过在国内外招募计算机高手，已经建立起一支“黑客部队”。这支部队训练有素，接到命令后随时可发起信息网络攻击，入侵别国网络，进行破坏、瘫痪甚至控制。最后，组建信息网络战

进攻部队。美国空军在2007年组建了一支专门负责实施信息网络进攻的航空部队——空军网络司令部。布什时代的网络安全战略重点在于“攻防结合”。

### 1.3. 奥巴马时代的网络安全主题：网络威慑

2009年2月，奥巴马指示美国国家安全委员会和国土安全委员会负责网络空间事务的主管梅利萨·哈撒韦组织对美国的网络安全状况展开为期60天的全面评估。经过几个月的工作，2009年5月，奥巴马公布了名为《网络空间政策评估——保障可信和强健的信息和通信基础设施》(Cyberspace Policy Review——Assuring a Trusted and Resilient Information and Communications Infrastructure)的报告，并发表重要讲话。奥巴马在讲话中强调，美国21世纪的经济繁荣将依赖于网络空间安全。他将网络空间安全威胁定位为“我们举国面临的最严重的国家经济和国家安全挑战之一”，并宣布“从现在起，我们的数字基础设施将被视为国家战略资产。保护这一基础设施将成为国家安全的优先事项。”

同时，不断完善美国信息网络安全组织机构。2009年5月，奥巴马发表声明，决定将成立白宫网络安全办公室，其办公室主任将担任白宫网络安全协调官。2009年6月，国防部长盖茨根据奥巴马决定，发布备忘录，宣布正式成立由国防部国家安全局局长领导的美国网络司令部，统一领导军事网络空间战活动。2009年12月，美国总统奥巴马正式任命白宫网络安全顾问霍华德·施密特为“网络沙皇”，担任白宫网络安全办公室主任一职。2010年5月23日，美国国防部宣布，美国网络司令部正式启动，由国家安全局长基思·亚

历山大任司令，将与国土安全部、国家安全局等部门密切合作，打击敌对国家和黑客的网络攻击，协调网络安全以及指挥网络战，以便有效维护美国信息网络安全。

奥巴马上台后采取了两个重要决策：第一，削减了包括 F22 战机在内的传统武器；第二，大幅增加网络攻击武器的投入。美国的战略重点正从实体战场逐步转向网络，“实体消灭”转到“网络瘫痪”。美国是世界上第一个引入网络战概念的国家，也是第一个将其应用于战争的国家。奥巴马政府的网络安全战略重点为“攻击为主，网络威慑”。

2011 年 5 月，《网络空间国际战略》的发表标志着美国网络安全国家战略已经完成从防御到攻击、从国内到国际的转变，但无论怎么变化，都是以美国国家安全战略为指导，服务于美国国家利益。

## 二、《网络空间国际战略》组成结构

《网络空间国际战略》以“基本自由、隐私、信息的自由流动”作为核心原则，努力去建设一个开放的、互操作性强的、安全可靠的未来网络空间，着重阐述了网络保护、网络治理和网络对抗，共设置了四部分内容。

第一部分是构建网络空间策略，该部分阐述了构建网络空间的战略探索，分别为构建于成功之上、认清挑战、基于原则。构建于成功之上，美国致力于维护和加强数字网络为社会和经济发展所带来的利益，美国承诺保护和提升数字网络为美国的社会和经济带来的利益；认清挑战，“数字基础设施已经越来越成为繁荣的经济、活跃的研究社区、强大的军事、透明的政府和自由的社会之脊梁”，美

国认识到网络的发展给美国和国际社会的经济安全带来了新的挑战；基于原则，美国将面对这些挑战——同时基于美国在网络空间问题上意欲保护的三个核心原则：基本自由、隐私和信息流动自由。

第二部分是网络空间的未来。首先，描绘了未来的网络空间：开放和互操作性的网络空间，安全可靠的网络空间，保稳定的国际行为准则下的网络空间。未来网络空间应当具备 4 个关键特征：1，开放促进创新；2，互操作性确保全球的覆盖；3，安全足以赢得人们的信任；4，可靠足以支持人们的工作。其次，定义了美国在未来网络空间中角色：为了实现这个未来网络空间，并积极推进规范和准则，美国将从外交、国防和发展三方面来提高网络的繁荣性，安全性和开放性。加强伙伴关系，包含双边和多边的伙伴关系，包含国际组织和多干系方组织，包含私营机构；防御和威慑，加强本土防御与海外防御，建立全球性的事件响应能力，如果犯罪分子对美国的网络进行攻击，必将承担惩罚风险，强调了网络空间的“集体自卫”、集体威慑能力和集体安全；建立繁荣与安全的网络空间，构建技术能力、构建网络空间安全能力、构建政策关系。

第三部分是政策优先。为了建立和维持开放、兼容、安全、可靠的网络环境，需要相应的政策支撑，它们分别是：1，经济：推动国际标准和创新的开放市场，确保网络空间继续满足美国的经济和创新的需要；2，保护美国的网络：加强安全、可靠性和容忍度；3，法律执行：拓展合作和法律力度，提高网络空间的信心，追究破坏在线系统者；4，军事：准备应对 21 世纪安全挑战，承诺在可能受到威胁的地方捍卫美国的公民、盟友和利益；5，互联网治理：推动

有效和包容的多样结构；6，国际发展：构建能力、安全和繁荣，在全球范围推广网络技术，提高共享网络的可靠性，在网络空间中构建有责任的参与者的大社区；7，互联网自由：支持根本的自由和隐私，在网络空间中，保护基本的自由和隐私。

第四部分为继续前进。进行了简单总结，指明：该战略为美国政府部门和机构更好的界定和协调在国际网络空间政策中所扮演的角色提供了路线方针，更有利于未来工作的开展和规划的实施。网络的利益不应局限于少数国家，而应当服务于广泛的世界，私营机构、民间社会、最终用户应当参与进来，与美国有共同认识的国家应当参与进来。

其中，第三部分政策优先是整个网络空间国际战略的重要基础，对于理解美国网络空间国际战略将起到至关重要的作用。

### 三、战略重点内容解读

为了推行美国的意识形态和国家霸权，服务于美国国家安全战略，以美国信息网络安全建设国家战略为指导，美国《网络空间国际战略》采取遵循基本原则（基本自由、隐私和信息流动自由）的方法，以总体目标（在

国内外建立和维持开放、兼容、安全、可靠的网络空间，捍卫美国的公民、盟友和利益）为导向，由经济、文化、技术、法律、军事和外交等方面的政策所支撑，它们共同形成了美国的网络空间国际战略的基础。下面主要从技术角度对美国网络空间国际战略的相关重点内容进行解读。

#### 3.1. 应对挑战

全世界必须共同认识到恶意为者进入网络空间带来的严峻挑战，并相应的更新和增强国家和国际策略。美国认识到网络的发展给美国和国际社会的经济安全带来了新的挑战，例如，自然灾害和事故破坏美国的电缆、服务器以及无线网络，一个国家屏蔽网站的方法会引发更大的国际网络破坏，勒索、欺诈和剥削儿童威胁用户在在线商务和社交网络方面的信心，甚至是他们的人身安全，对知识产权的窃取威胁到了国家的竞争力和创新能力。随着传统的冲突形势延伸进入网络空间，更广泛的来看网络安全威胁甚至危及到了国际的和平与安全。这些挑战已经超越了国界，进入网络空间的低成本以及建立匿名的虚拟身份为罪犯提供了“安全的避

所”。

为了应对这些新的挑战，美国致力于国际倡议和标准，加强网络安全并同时维护自由贸易和信息自由流动。国际上最好的工程师一起工作，开发新标准和信息系统，使网络更快，更可靠，更具创新性和无缝性。高新技术企业与他们的客户一起工作，可以提供更安全、更可靠、更符合客户需求的软件、硬件和服务。大学和企业可以自由的研发新概念和新产品。当网络安全事件需要政府干预时，官员可以尽早的检测威胁，实时的共享数据，阻止恶意软件的传播，最大限度的降低破坏程度，同时也能维持信息不间断传输。当涉及到国际犯罪调查时，执法机构能够进行跨国合作，维护和分享证据，并把罪犯绳之以法。在网络空间里，国家要负起责任，不遗余力防止他人破坏网络，还要剥夺犯罪分子的避风港。国家必须加强对网络基础设施的尊重，使得国家争端不会成为干扰甚至破坏网络的借口。

#### 3.2. 安全可靠的网络空间

网络的稳定性是全世界繁荣昌盛的基石，一个有效的政策往往需要从各个方面采



取行动，由社会各阶层共担责任，并通过各个国家的最终用户开展合作。对于网络的管理绝不能仅限于政府，而应包括所有的利益相关者，即多方管理。网络空间必须是安全可靠的，它们必须依赖于信任的个人、企业和政府，能够有效的抵御任意或恶意的破坏。

降低网络的脆弱性需要强有力的技术标准和解决方案、有效的事故管理、可信的硬件和软件以及安全相关的供应链。事故响应需要加强私营机构和国际社会双方的合作和技术信息共享。由于网络的核心功能依赖于可信任的系统（如边界网关协议），各国必须承认其技术层面的决策会造成国际影响，并尊重彼此的网络和国际互联网。同样，在设计下一代网络系统时，我们必须依靠健全的技术标准和管理结构去实现共同利益。减少网络侵入和破坏，避免未经授权的网络入侵威胁各经济体的完整性和破坏国家安全。美国政府部门将与私有机构合作，保护科技创新，防止工业间谍活动，并确保关键基础设施的安全以防入侵和攻击，特别是在能源、运输、财务系统以及国防工业基地。提高信息基础设施事件管理能力和恢复能力，增强灵活性。通过行业咨询，提高高新技术产业供应链安全性。

加强全球网络空间治理一直是世界各国的共同愿望和要求，互联网虽然是美国人发明的，根服务器也大多控制在美国人手中，但是互联网这些年来的迅速发展则是国际社会共同努力创造的成果，是人类共同的财富，也是促进世界和平与发展的新空间。制定关于网络空间的国际政策，应该是全世界的事情，也应严格遵循《联合国宪章》和其他国际公认的基本准则，在维护本国信息领域国家主权、利益和安全的前提下，依据联合国、国际电信联盟有关决议和相关

国际公约，和平利用国际信息网络空间。只有这样，才能促进网络空间和网络经济的健康发展，维护世界的和平与繁荣。

### 3.3. 劝止和威慑

美国将捍卫自己的网络，无论是来自恐怖分子、网络罪犯还是来自其他国家及其代理人的威胁，将设法鼓励良好行为并劝阻和制止那些在网络上威胁和平与稳定的行为。美国反对破坏网络和系统的行为，劝阻和制止恶意行为，并保留采取必要和适当措施的权利来保护这些重要国家资产。

保护如此之大价值的网络需要很强的防御能力。美国将继续增强美国的网络防御、承受和从其它攻击中恢复的能力。对于那些造成严重损害的攻击，美国将采取行动来隔离和减少对设备的干扰，降低对网络的以及潜在的级联式的影响。十年来，美国已经形成了一种网络安全文化，研制了对风险事件有效缓解的设备。无论是对公共部门还是对私营部门，采用良好信息技术的系统将减少美国的脆弱性并增强网络和系统。美国已经建立了安全事件响应小组，在政府、重点行业、关键基础设施部门和其他利益相关者之间共享信息。此外，美国不断寻求新方式来加强与私营企业的伙伴关系，以加强安全性。拒绝服务攻击对美国和国际网络造成持久的损害，全球分布式网络需要全球分布式预警能力，必须继续在全球范围形成新的计算机安全事件响应能力，并帮助发展中国家加强计算机网络互连和防御能力。

对网络攻击要阻止和威慑并举，强调网络空间的“集体自卫”、集体威慑能力和集体安全，美国将继续在军事和民间领域与美国的

盟国和伙伴共同努力，拓展态势感知并共享预警系统，以提高在和平或危机时期携手合作的能力，以及发展在网络空间集体自卫防御的方法和手段。必要时，美国将会对网络空间中敌对行为作出回应，就像美国回应对美国的国家其他威胁一样。所有的州都拥有自卫权利。为了保卫美国、美国的盟友、美国的合作伙伴和美国的利益，美国保留使用一切必要手段的权利——外交、信息、军事、经济、以及适当的和适用的国际法律。

#### 四、网络空间国际战略对我国的启示

美国政府出台《网络空间国际战略》，意图以美国价值观引领全球网络发展，夺取网络空间的信息主导权，其背后有着全面而长远的战略考虑。美国《网络空间国际战略》的发布，将网络空间的主权、利益与安全问题推到了我们面前。目前，我国尚未从国家层面制定具有统筹性和前瞻性的网络空间发展战略，也缺乏网络空间发展、管理和安全方面的法律法规。在这样严峻的形势下，中国必须提高对网络空间重要性的认识，认清和把握网络空间国际战略形势，充分考虑我

国国情和信息技术发展现状，采取有效措施积极应对，快速探索出一条具有中国特色的网络空间建设之路。

（一）尽量避免为美国《网络空间国际战略》所牵制，加紧制定符合中国国情的网络空间战略

《网络空间国际战略》是美国第一次公开针对网络空间制定的全盘计划，也是第一次把美国国际政策目标与网络空间政策结合在一起，其内容与目标已从美国自身的网络空间范围扩展到全球网络空间。美国单方面制定全球网络空间未来的发展、治理与安全战略目标，使得各国尤其是我国在网络空间中的政治和价值观受到巨大冲击。为应对挑战，中国应结合自己的国情，尽快从国家层面制定具有统筹性和前瞻性的我国网络空间发展战略，引导政府、企业、个人等社会主体积极参与我国网络空间建设，避免在网络空间国际活动中处于被动。

（二）加紧研发网络新技术、新应用以及信息安全防御技术，构建完善可靠的信息网络安全防护体系

美国《网络空间国际战略》预示着网络

将再次成为国际社会争夺的焦点。美国将凭借在信息技术领域的优势力促发展中国家进一步开放信息技术、产品与服务市场。在网络自由问题上，美国会将人权问题与之挂钩，大力推广破解技术，敲开一些发展中国家网络信息传播的大门。以针对他国重要信息系统和网络基础设施等为主要攻击对象的“网络战”将成为国际战争新的形式。我国应加强对国外先进网络技术和应用的跟踪研究，同步研究网络安全漏洞检测和预警技术，评估并提高我国网络安全纵深防御能力。同时，应加大国产自主可控技术和应用的研发力度，鼓励网络安全企业发展创新，使我国用户依赖的网络安全技术掌握在自己手里，避免依赖他人的被动局面。

（三）推动国际合作与对话，积极参与国际网络标准与规则的制定工作，创建积极向上、阳光绿色的网络环境，构建健康的网络传播秩序

美国国务卿希拉里在白宫首次展示《网络空间国际战略》政策文件时称，各国必须为网络空间制定“大家都能接受的”国家标准。美国《网络空间国际战略》中也明确，美国

致力于制定公认的国际协议和新标准，加强网络安全并同时维护自由贸易和信息自由流动。同时，将“推动国际标准”列为日后美国在网络空间着力推进的7大政策重点之首。这一系列做法都显示出美国政府掌握全球网络发展与安全标准及规则主导权的决心，并希望通过制定带有美国式价值观的国际规则来确立其在网络空间的霸主地位。我国应提高对网络空间技术及管理国际标准的重视，积极推动国际合作与对话，参与制定国际网络标准与规则，改变我国在国际标准制定方面的被动局面，提升国际话语权，增加我国在未来网络空间新格局中的分量，进而维护国家主权和人民利益不受侵犯。

(四) 加强政府部门与信息产业界的联合协作，建立健全我国网络空间发展、管理和安全方面的标准法规

美国建立了一系列信息安全方面的标准法规，制定了信息安全建设国家战略，健全了信息安全标准法规体系。2009年5月29日，奥巴马公布了名为《网络空间政策评估——保障可信和强健的信息和通信基础设施》的报告，强调美国21世纪的经济繁荣将依赖于网络空间安全，并介绍了信息安全相关法律和法规框架的制定情况。2010年12月，美国国家标准技术研究院公布了名为《对联邦信息系统和组织进行信息安全持续监控》(Information Security Continuous Monitoring for Federal Information Systems and Organizations)的技术规范。2011年7月，美国国防部又发布了《网络空间行动战略》(Strategy for Operating in Cyberspace)，解决了如何认识和理解网络空间战略的概念框架问题。美国在信息网络方面采取的一系列举措，提示我国要加强国

家层面的信息网络安全统一领导和协调，加强政府部门与信息产业界的沟通和协作，进一步健全我国的信息网络安全标准和法规，加强信息安全、网络安全、数据安全等网络空间方面的立法工作，明确界定网络空间违法违规行为，使我国网络空间发展和管理有法可依，任何个人、企业甚至其他国家在我国网络空间中必须依法活动。

#### 参考文献:

- 1、The White House. International Strategy for Cyberspace. [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/international\\_strategy\\_for\\_cyberspace.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf)
- 2、The White House. Cyberspace Policy Review(Assuring a Trusted and Resilient Information and Communications Infrastructure). [http://www.whitehouse.gov/assets/documents/Cyberspace\\_Policy\\_Review\\_final.pdf](http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf)
- 3、The White House. International Strategy for Cyberspace Fact Sheet. [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/International\\_Strategy\\_Cyberspace\\_Factsheet.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf)
- 4、Peter H. Chen. The Strategic Evaluation of the National Strategy to Secure Cyberspace. <http://www.peter-chen.com/docs/IWPaper.pdf>
- 5、陈晓桦，左晓栋. 美“国家网络安全综合计划”揭开神秘面纱. 信息安全与通信保密. 2010(4)

# 银行各类部门 在IT风险管理体系中的职责

行业技术部 徐一丁

**摘要：**介绍银行常见的各类部门在IT风险管理体系中的职责。IT风险和信息安全是全行各部门的共同责任，根据部门的本职工作不同而有所区别。

**关键词：**银行风险管理部门职责 商业银行风险管理体系 银行IT风险管理 信息安全

## 引言

绿盟科技长期为各大行业客户提供安全服务，在为银行业金融机构进行IT风险管理咨询中，发现银行各部门人员对IT风险防范和信息安全管理都有一定认识，但又不清楚自己到底应该做些什么。本文介绍了银行各部门开展这项工作的思路。

## IT风险管理“三道防线”

银监会《中国银行业“十二五”信息科技发展规划监管指导意见》（征求意见稿）中要求：“建立并完善信息科技部门、信息科技风险管理部门、信息科技审计部门“三道防线”，分清职责、理顺流程、落实岗位责任制，形成完备的管理、监督和问责机制。”

根据指导意见，银行可以考虑建立以下形式的“三道防线”：

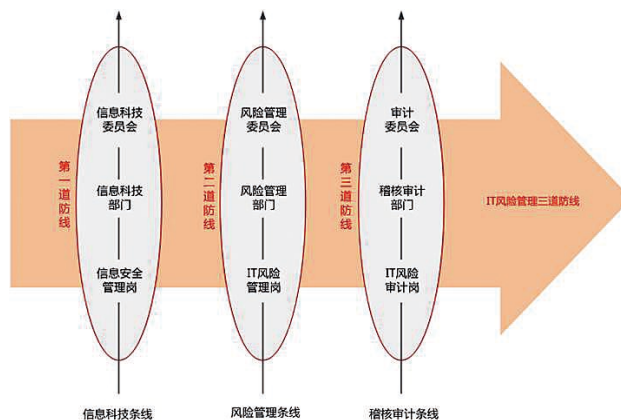


图1 银行IT风险管理“三道防线”

信息科技部门

信息科技条线整体负责第一道防线，由上至下为信息科技管理委员会-科技信息部-信息安全管理岗。第一道防线中，信息科技部门根据信息科技委员会的 IT 治理整体方针，制订信息安全方针策略和相关制度，日常 IT 风险防范和信息安全保障措施的具体落实，做好安全防护的事前预防、事中响应处理和事后总结改进的工作。

#### 风险管理部门

风险管理条线整体负责第二道防线，由上至下为风险管理委员会-风险管理部门-IT 风险管理岗。理想状态下，风险管理部门管理银行全面风险管理工作，IT 风险是其管理职责的一部分。IT 风险纳入到操作风险，最终纳入到全面风险管理体系中去。第二道防线中，风险管理部门应负责 IT 风险管理策略的制订，定期执行评估，对银行 IT 风险进行动态的计量与动态监控，根据监督执行。

#### 稽核审计部门

稽核审计条线整体负责第三道防线，由上至下为审计委员会-稽核审计部门-IT 风险审计岗。第三道防线中，稽核审计部门应根据已有的审计准则，制订 IT 审计策略，

定期实施 IT 风险和信息安全状况的审计，及时发现相关工作的不足，提出改进意见和建议，并监督执行。

IT 风险管理“三道防线”，充分体现了银行高度重视风险管理和权力制衡的思想，这三个部门也是 IT 风险防范的核心部门。然而其他部门也在 IT 风险和信息安全管理体系中起着重要的作用，下面我们进行简要说明。

#### 业务部门

银行常见的业务部门，无论资产、负债还是中间业务部门，一举一动都涉及到资金，责任重大。并且业务部门工作中对 IT 系统的依赖程度都很高，银行已经是一个高度 IT 化的企业。这种情况下，业务操作风险就与 IT 风险紧密地结合起来。业务部门应依据“最小权限原则”，将业务权限层层进行分解，然后充分利用 IT 技术层层进行控制，包括身份认证、授权和操作审计。

银行常见的身份认证方式有电子证书、磁条卡和指纹，电子证书基本用于内部业务处理，磁条卡和指纹认证由于操作方便，也可以同时用于柜面和外部业务。业务管理系统

确认操作者的身份之后，赋予其相应的业务权限，并对后续操作进行记录，以备事后的行为审计。

这套认证授权的机制在各银行都运用得比较成熟，作为银行业务人员就应保管好自己的身份认证凭据，如电子证书、磁卡等。认证凭据被盗用等于身份被盗用，不但可能给银行带来损失，还会给自己带来麻烦。

#### 人力资源部门

人力资源部门通常负责银行的人事管理与人力规划、工资薪酬、绩效考核、员工招聘、调动和培训等工作。我们在调查中发现，很多银行的人力资源部门都没意识到自己在信息安全和风险控制方面应负的责任。

信息安全体系的三个维度中，组织、制度、技术中，最难达到理想状态的往往是组织这个维度，也就是人员的组织，最不容易防范的也是内部人员的恶意和违规行为。内部人员清楚地了解银行的基本情况，工作流程，可以很容易地找到内部的各方面漏洞而加以利用。另外，内部人员由于知识经验的原因，还可能出现危险操作和失误的操作，同样会给业务带来严重损失。

在实际环境中，内部人员的攻击或误操作是不可能通过 IT 措施来 100% 防范的，因此银行需要加强人员安全的管理，而这方面的主要责任应由人力资源部门承担起来。

人员从应聘到上岗的全过程中，人力资源部门应协调各方面对该人员进行审核，全方位衡量该人员是否适合从事该岗位的工作，包括知识、技能、经验、素质、操守等。所以除了知识技能考核，还要做人员背景调查。员工上岗时，人力资源部门应安排员工与银行签订专门的保密协议，确保员工遵守安全和保密规定。

人员在离职或转岗的时候，应注意做好其相关系统使用权限的变更，避免违规操作。常见的 IT 权限包括系统账号、密码、文件服务器权限、各类系统权限、E-Mail 账号、电子证书、磁卡等。人力资源部门应委托专业人员，通常是 IT 部门的系统管理员完成这些权限变更，人力资源部门应确认这些变更已经实施。

员工的一进一出做好控制了，日常的安全和意识培训也要进行，以避免员工在履职期间出现有意或无意的问题。除了计算机安全操作知识外，对年轻的员工还应注意进行人生观和价值观的教育。曾经有一位银行业内的人士谈到：“现在的年轻人没有经历过原来我们的艰苦环境，从小也都在比较舒适的生活里长大，性格随意，责任感普遍不强。进入银行之后，工作态度不能适应银行严谨工作的需要，经常出错。更有甚者，业余生活中抵御不住各种诱惑，参与赌博或花钱无度，而他们每天在银行里都面对巨额资金，很难不出问题。所以我们觉得政治思想教育仍然非常重要。”——这说得太好了。

另外还要注意外包人员的问题，银行经常忽略这方面的安全隐患。外包人员的资质背景同样需要审核，外包公司更换人员需要经过银行同意，外包人员同样要签署保密协议，并参加必要的培训。

---

### 办公室

---

办公室通过负责公文管理，可以进行纸介质信息的安全管理。现在很多银行推行“无纸化办公”，但还是有很多银行的工作中涉及到大量纸介质的信息，如红头文件、会议通知、各类记录、内部通讯录……银行通常有严格的内部控制机制，但在纸介质信息的管理方面还是存在着很多疏漏。如员工桌面随意放着通讯录的小本子，内部的主要部室、人员在上面都有记载。我们还曾经在银行复印室的废纸箱里发现撕成两半的废弃合同。

所以纸质文件的安全管理还是应该有个部门来负责的，办公室比较合适。

---

### 安全保卫部门

---

提到安全保卫部门，想起朋友的一条微博：今天上午到公司，在我进入大门时被保安拦住，被问了三个哲学上的终极问题：“你是谁？”“你从哪里来？”“你要到哪里去？”——在大笑之余，发现这确实是咱们国内保安人员问得最多的三句话。

安全保卫部门负责保护银行的物理安全，其重要性不必多说，还是谈谈存在的主要问题。管理比较严格的银行（通常为全国性银行），进入重要的楼宇之前，每次都要先登记再进入。而地方性银行，即使是总部或核心机房所在的大楼，很可能对保安人员说“我找某某部门的某某人”，就被允许进入。多次进出熟悉之后，甚至

## ► 行业热点

---

向保安人员点点头就行了。在大楼比较松散的物理控制条件下，一般只有进入核心机房时才需要登记、签名等。其实银行除了机房之外，还有很有 IT 相关环境中保存着重要的信息，同样需要物理安全的保护。

---

### 信息科技部门

---

再回过头来，说说信息科技部门的重要责任：研究制订适合本银行情况的信息安全策略和制度，并推行落实到全行。我们在访谈的时候，银行其他部门总是说：啊，确实没意识到信息安全方面还有这么多漏洞。但大家同时也挺委屈，觉得自己不懂，也从来没有人告诉他们这些风险。IT 技术专业性很强，信息安全知识与意识的建立，主要应靠信息科技部门来主导，安全制度最好能与其他部门一起制订，再由各部门去落实执行。

还应注意，银行各部门的安全工作其实是有相关性的，并不孤立。我们假设一个场景：某个银行的新员工，没有受到必要的安全保密教育，缺乏安全意识，把银行发的通讯录随意地携带，在外面丢失了。通讯录被别有用心的人得到，从上面了解到了银行内部的组织和人名，于是他大模大样地来到银行大楼，对保安人员说“我找信息科技中心的某某”，就被放行了。他堂而皇之地在大楼里四处参观，同时看看是否有机可乘，结果在复印室里找到了更多被废弃的有价值的资料 and 文件……所以信息安全关系到每个部门，大家都责任把自己这个环节把控好，并不断完善，才能形成真正良好的信息安全环境。

# 软件自动化测试实践

研发二部 李志昕

**摘要：**在软件行业，软件测试相对来讲起步较晚，但发展还是比较快速的。目前，大多数软件相关的企业，都已经配备有独立的软件测试团队。同时，在软件研发规模的迅速扩张及软件生命周期的逐步压缩的双重压力下，如何提高研发效率的问题便突显出来，软件自动化测试便是解决这一问题的重要手段之一。但是，企业在不同的发展阶段，能够对自动化测试的投入可能也是不同的，本文将主要介绍在不同的阶段如何引入和实施自动化测试。

**关键词：**软件测试 自动化测试 实践

## 一、前言

软件自动化测试是目前软件测试行业中比较热门的一个方向，相关的有对方法的讨论、有对工具的研究，本文不希望对此作以综述性的介绍，而更多是从自身的实践经历出发，阐述随着企业的发展，自动化测试从无到有再到壮大的过程，可能会给有相似背景的同行一些启发。

进入正文之前，做一点说明，本文主要讨论的是“软件自动化测试”，后续为了描述方便，简称为“自动化测试”。

## 二、自动化测试的理解

自动化测试不是指测试的某个阶段，而是相对于手工测试来讲的一种测试方式，所以自动化测试可以贯穿于产品研发的各个环节。反之，如果过于强调一定在某个阶段集中去做自动化，实际上则可能达不到预期的成果。这一点似乎看起来过于浅显了以至于不需要去强调它，但实际当中这种做法很普遍。本文后面讲述的实践过程则是以此为理论基础。

自动化测试本质上是编写程序测试另一个程序。这一定义还是被普遍接受的，那么由此得知，自动化实现的过程与产品开发的进程并无二致。也就是说，自动化测试的关

键并不在于脚本的编写，测试需求分析、测试脚本设计更加重要。同时，好的自动化还会考虑到可复用性、可维护性等等。不过，理论上虽然是这样讲，真正实施的时候，如果限于资源不足等条件，还是可以先以实用为首要原则。

## 三、半自动化测试

往往在企业发展初期，测试团队规模比较小，此时要做完全的自动化测试可能是不现实的。这个阶段更多的是依靠测试人员自发的实现一些自动化工具，来辅助测试的执行，不妨称为“半自动化测试”。简单分析一下两者的区别（见表1）。



	半自动化	全自动化
测试数据	(1) 脚本中固化 (2) 命令行	数据文件 (txt、xml、excel) 数据库
测试操作	大部分由脚本完成，小部分由人工介入	全部由脚本完成
测试结果	部分中间结果由脚本处理，最终结果由人工判断	全部由脚本判断
输出 (操作返回结果、日志)	输出到屏幕	输出到文件
异常处理	不做异常处理，出错了手工调试	需要做异常处理，考虑各种情况，避免脚本停止运行
复用	代码复用 (拷贝)	模块复用 (调用)
测试范围	单一测试	集合测试

表 1 半自动化与全自动化测试对比

可见，半自动化的主要不足是需要人工的参与，即便如此，还是会很大程度提高测试执行的效率。比如重复的操作由脚本完成，输出结果稍做格式化的处理便可大大方便测试结果的分析 and 判断，而且因为不用考虑太多异常的处理，开发成本也不高。通常情况下，使用 Windows 的批处理及 Linux 的 shell script 就能够实现很多自动化测试功能。

举一个例子，测试需求是：验证由安全中心下发给安全设备的策略是否正确。思路是：对比下发到设备上的策略文件和安全中心本地的策略文件的 MD5，验证是否一致。图 1 是 Windows 批处理

脚本 “policy.bat”：

```

1 @echo off
2
3 set addr=%1
4 set nsmdir=c:\Program Files\nsc\
5 set rules=p1.xml p2.xml p3.xml p4.xml
6
7 for %%i in (%rules%) do if not [%%i]==[] (
8     echo %%i
9     wget https://%addr%/getPolice?rule=%%i -O %%i
10)
11
12 for %%i in (*) do if not [%%i]==[] (
13     echo -----
14     md5sum %%i "%nsmdir%\%%i"
15)

```

图 1 policy.bat 脚本

这个脚本就符合上面提到的“半自动化”的基本特点，可以看一下脚本的执行的结果 (见图 2)。

```

c:\>policy.bat
"p1.xml"
0b40b92cb609c43c1bc19f9403c22fce *p1.xml
\0b40b92cb609c43c1bc19f9403c22fce *c:\Program Files\nsc\p1.xml

```

图 2 policy.bat 执行结果

由该打印输出，已经可以比较直观的看出策略文件是一致的。

#### 四、自动化测试框架

当企业发展到较大规模时，对自动化测试的投入自然也会成比例的增加，此时可能会出现自动化测试框架的需求。毕竟依靠测试人员自发的、零散的自动化测试起不到规模效应，而且很可能导致不同产品自动化测试过程中会重复开发相同功能的脚本，也就是我

们常言的“重复造轮子”。

此时我们又会来到一个十字路口，是自主开发一套测试框架，还是买一套测试工具呢？通常我们阅读自动化测试方面的书籍，都会发现有一章专门讨论如何进行工具选型<sup>[1]</sup>。买，自然是花费很高，自主开发，实际上投入也很可观。其实还有一条路可能读者也想到了，就是利用开源或免费软件。例如：Web 测试有 selenium、watir，Windows 测试有 Autolt，性能测试有 Jmeter 等等<sup>[2]</sup>，而且这些免费测试工具的发展真的是非常快。

不过，本文并不是要介绍这些免费工具的使用，而是想讨论利用这些资源整合形成自己的测试框架。如何整合呢？其实说出来没有什么特别，就是利用脚本语言。我们目前选择的是 Python 语言，那么 selenium 本身就提供 Python 的 API，而 Autolt 可以通过 Com 接口去调用。即便没有提供 API，使用 CLI 也没有问题。记得 Perl 曾经被称为胶水语言，或许可以说 Python 也具此特性。

有了 Python 这个强大武器，再整合众多的免费测试工具，只要互相有效配合，就能够实现绝大多数的自动化测试了。只要在此

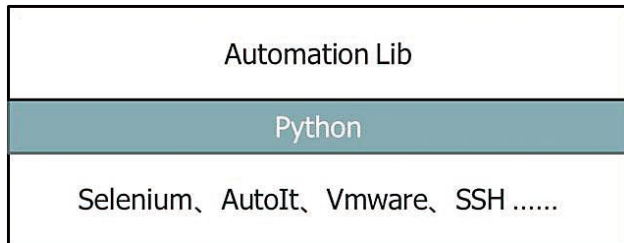


图 3 自动化测试框架主体结构

基础上根据自身的需要再进行一层封装，提供相对简化方便调用的接口，这样框架的雏形就形成了（见图 3），可以满足有组织的自动化测试初期的需要。

#### 4.1 自动化测试平台

框架的意义不应仅是提供一组库，更重要的是提供脚本开发规范和模式，再加之自动化执行过程的管理，由此便形成了自动化测试平台<sup>[3]</sup>。

自动化测试平台首要解决的，不是功能如何强大，而是易于测试人员应用。此时的测试人员成为了客户，如果难于上手，客户就可能放弃使用。例如 QTP，其支持的“关键字驱动”的脚本开发模式，允许不懂编程的人也能够实现自动化脚本。要不要也按这个思路去做？这又是一个令人纠结的问题。

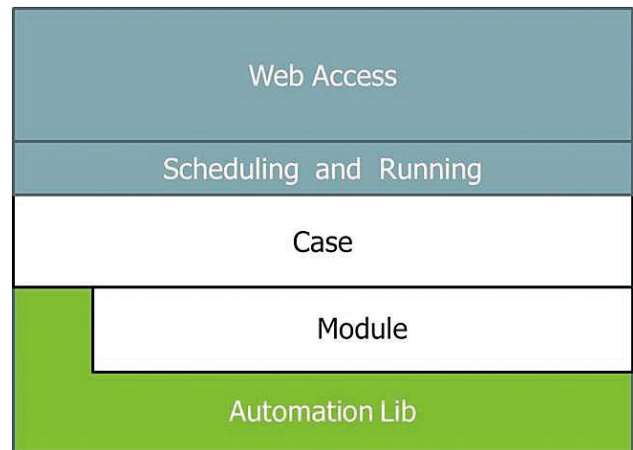


图 4 自动化测试平台主体结构

此时我们再回顾一下前边提到的自动化测试的本质，似乎在提示，不要偏离编程这条航线。那么再思考一下，Python 语言属于比较容易学习的语言，为何不让测试人员都掌握 Python 呢？让我们再规划一下自动化测试平台的架构吧（见图 4）。

这里把自动化测试脚本的实现分成两个层次 Case 和 Module。Module 主要实现对被测软件操作的模拟、异常处理等，Case 主要实现测试流、测试数据。自动化框架可以提供数据驱动的功能，编写 Case 只需要调用 Module 提供的方法完成测试流就可以了。请看下面的示例：

测试需求：验证安全中心在正确配置时添加用户是否成功。

首先定义安全中心 Module（暂时不管 selenium 使用的细节）

nsc.py（源码见图 5）。

```
1 import selenium
2
3 class userMgmt:
4     def __init__(self):
5         self.sel = selenium
6
7     def new(self, name, passwd, vpasswd):
8         ...
9
10    def edit(self, name):
11        ...
12
13    def getList(self):
14        ...
15        return userList
```

图 5 nsc.py 脚本

再看测试用例脚本 testNsc.py（源码见图 6）：

```
1 import unittest
2 import nsc
3
4 class testUserMgmt(unittest.TestCase):
5     def setUp(self):
6         self.uM = nsc.userMgmt
7
8     def testAddUserSuccess(self):
9         self.uM.new("Gerald", "123", "123")
10        uL = self.uM.getList()
11        self.assertEqual(ExpectUL, uL)
12
13    def tearDown(self):
14        pass
```

图 6 testNsc.py 脚本

“ExpectUL”是预先定义好的预期结果。这样看来，编写 Case 就比较容易了。测试人员剩下要做的就是通过 Web 对 Case 的执行进行管理，分析测试报告。

#### 4.2 自动化测试开发

细心的读者可能发现其实前边回避了一个问题，就是测试 Module 的实现。的确，Module 的实现是最为复杂的，编写 Module 不仅要精通编程和测试工具的使用，对被测软件也需要有一定的理解。要理清这处要害，还要从组织结构着眼，也就是要不要有专门的自动化测试工程师？实际上，编写 Module 对程序设计能力的要求还是要高于对被测软件的理解。恰与编写 Case 相反，编写 Case 需要对被测软件和测试方法理解更多。这样可以看出分离 Case 和 Module 的实现，实际上达到了精通编程和理解产品的融合。

那么现在再回到最初提出的“自动化测试贯穿研发各个环节”，

	开发人员	自动化测试人员	测试人员
需求分析		提出自动化测试需求	
详细设计	为自动化测试提供接口 (API、CLI、文本接口等) 提供界面原型, 规范使用元素名称或 ID	沟通确定自动化测试接口定义	沟通确定测试 Case 与 Module 接口定义 设计自动化测试用例
编码	遵守设计约定, 实现自动化测试接口, 如需变更则通知测试人员 单元测试	遵守设计约定, 部分实现自动化测试 Module 编写	遵守设计约定, 部分实现自动化测试 Case 编写
集成测试	集成测试	自动化测试脚本联调	
系统测试	补充 Module 编写		补充 Case 编写 执行自动化测试
维护	提供支持		负责持续更新

表 2 自动化测试开发过程

看是如何进行的 (见表 2)。

从表 2 中我们可以看到, 在需求分析阶段, 测试人员就可以提出自动化测试需求。这种需求是为了后续方便实现自动化测试, 在产品设计和编码阶段为自动化脚本预留出调用接口。假设有这样一个测试需求: 验证 IDS 检测规则准确性。那么在需求阶段, 可以

提出相应的自动化测试需求: IDS 能够提供获取告警结果的接口。这样就不必从图形界面去获取告警信息, 实现自动化的难度将大大降低。当然, 能够恰当的提出自动化测试需求也是需要积累很多的经验的。

那么, 后续阶段的工作基本就是水到渠成了。有了设计约定, 则不需要等软件可运行, 部分自动化脚本就可以开始编写了。重点是要控制变更, 如果已知可能会频繁变更的, 还是尽量推迟脚本的编写, 或是在脚本设计时就能够适应变更。

这种自动化测试开发过程的优势就在于, 使自动化测试开发与产品开发能够并行, 使系统测试阶段的自动化程度有一定的提高。

### 五、结束语

自动化测试可以提高测试的效率, 能够增强测试的准确度, 但是自动化测试并不能够完全替代手工测试, 也不是解决软件质量问题的银弹。<sup>[4]</sup> 自动化测试过程中还会遇到很多需要具体解决的技术问题, 是一个值得不断去探究的领域。

### 参考文献

- [1] 朱少民, 《轻轻松松自动化》
- [2] Mark Fewster & Dorothy Graham 《Software Test Automation》
- [3] 柳胜, 《软件自动化测试框架设计与实践》
- [4] Addison Wesley & Pearson 《Automated Software Testing: Introduction, Management, and Performance》

# Adobe Reader X保护模式技术分析

研究部 赵亮

**摘要：**文章介绍了 Adobe Reader X 保护模式所使用的相关技术，讨论了各技术手段能够达到的功能和所受的限制。

**关键词：**保护模式 沙盒

2010年 Adobe 公司推出了 Adobe Reader X。Adobe Reader X 使用了保护模式 (Protected Mode, 又叫沙盒, Sandboxing) 来保护用户系统的安全。沙盒的主要思路是在一个受限的环境中 (沙盒进程, Sandbox Process) 处理潜在恶意的数据, 包括图像处理、Javascript 执行、字体 3d 渲染等, 所有需要在沙盒外进行的操作, 都需要通过一个代理进程 (Broker Process) 完成。沙盒进程和代理进程之间通过 IPC 进行通讯。图 1 是 Adobe Reader X 的软件结构图。

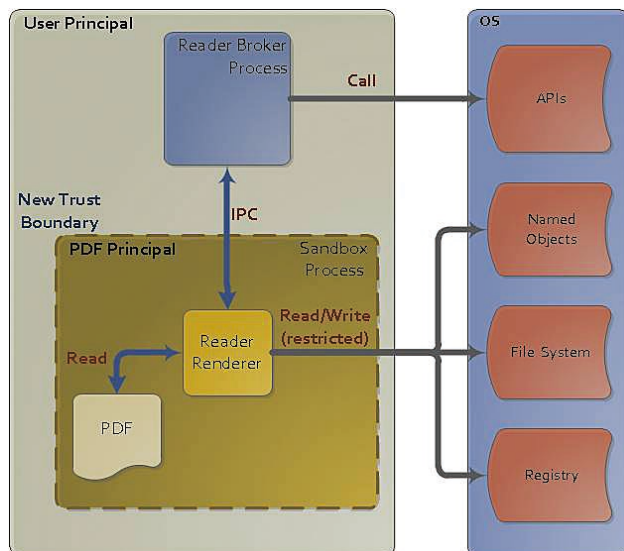


图 1 Adobe Reader X 的软件结构图

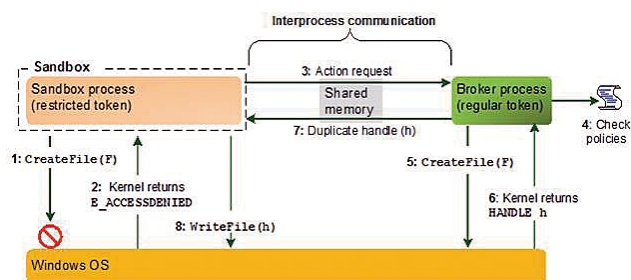


图 2 打开文件的流程

AdobeReader X 沙盒架构设计基于 Google Chrome 的沙盒, 并且参考了 Office 2010 的沙盒设计。目前在大型软件中使用沙盒还是一项比较新的技术, 现在使用了类似沙盒机制的软件包括 Microsoft Office 2007 MOICE、Google Chrome、Office 2010 Protected View 等。

Adobe Reader X 沙盒主要依赖操作系统的安全机制来实现, 同时遵守最小权限原则 (principle of least privilege)。首先, 由代理进程准备好受限的执行环境, 然后再在这个执行环境中启动沙盒进程进行数据处理。用 Process Explorer 可以看到代理进程和沙盒进程的父子关系。



 AcroRd32.exe	1172	Adobe Reader
 AcroRd32.exe	1284	Adobe Reader

图 3 代理进程与沙盒进程的父子关系

### 沙盒设计目标

Adobe Reader X 沙盒并不能保证不出现新的漏洞。沙盒的主要目标是在潜在的漏洞被成功利用后，降低恶意代码对用户系统的损害，主要体现在以下方面：

- 防止恶意代码向系统安装程序（释放可执行程序并添加注册表自启动项）；
- 防止删除系统文件，保护系统完整性；
- 防止修改系统配置；
- 防止键盘记录（需要 Windows Vista 以后版本）。

目前沙盒未对如下方面做限制：

- 对文件系统和注册表未授权的读操作，无法防止信息泄露；
- 网络操作完全不受限制；
- 剪贴板操作；
- 不安全的系统配置导致的影响。

### Windows 安全机制

Windows 系统提供的可用于沙盒的安全机制主要有以下 4 个方面：

- 作业对象 (Job Object)；
- 受限令牌 (Restricted Token)；
- 分离桌面；
- 用户访问控制 (UAC)。

其中对 UAC 的支持需要 Windows Vista 或以后的版本。出于安全性和实现复杂度的考虑，Adobe Reader X 沙盒目前没有使用隔

离桌面机制。

### 作业对象 (Job Object)

Windows 2000 开始提供了一个新的内核对象，作业对象。作业类似于 UNIX 里的 ulimit，它能够对作业内的进程所使用的资源做限制，例如处理器时间、内存总量、UI 对象的访问、作业内进程总数等。其核心函数是 SetInformationJobObject()，函数原型如下：

```

BOOL SetInformationJobObject(
    HANDLE hJob,
    JOBOBJECTINFOCLASS JobObjectInfoClass, // 限制类型
    LPVOID lpJobObjectInfo, // 根

```

限制类型	JobObjectInfoClass 取值	限制的内容
基本限制	JobObjectBasicLimitInformation // 2	进程用户态处理器使用时间，内存使用量，进程数量
扩展基本限制	JobObjectExtendLimitInformation // 9	包含基本限制和一些扩展
基本 UI 限制	JobObjectBasicUIRestrictions // 4	创建桌面，切换桌面，修改显示设置，注销，关机，访问 global atoms，访问 job 之外的用户 handle，读写剪贴板，调用 SystemParametersInfo
安全性限制	JobObjectSecurityLimitInformation // 5	安全信息

据限制类型不同，指向不同的数据结构，里面保存限制的信息

`DWORD CbJobObjectInfoLength`

//JobObjectInfo 的大小

通过这个函数可以设置对作业中进程的限制，其中 `JobObjectInfoClass` 指明了限制类型，根据 `JobObjectInfoClass` 取值的不同，`lpJobObjectInfo` 指向不同的保存限制信息的数据结构。

Adobe Reader X 通过作业对象机制对沙盒进程作了如下限制：

- 作业中进程数量为 1；
- 不能创建或切换桌面；
- 不能修改显示设置；
- 不能调用 `ExitWindows` 来注销或重启系统；
- 不能访问作业之外进程创建的 `USER Handle`；
- 不能通过 `SystemParametersInfo` 修改系统参数；
- 禁止作业内进程使用包含管理员组的令牌。

Adobe Reader X 没有通过作业对象对沙盒进程做如下限制：

- 剪贴板的读写；
- 访问 `Global Atom`；
- 内存、处理器的使用。

可以使用 `Process Explorer` 查看 Adobe Reader X 作业的限制：

作业中进程数量为 1 直接导致了 `exec` 类的 `shellcode` 的执行失败。有效地防止了恶意代码启动新的进程。

PDF 规范的一项功能就是执行一个系统命令，限制作业中进程数量为 1 会影响到 PDF 的这个功能，沙盒进程将不能直接执行被请

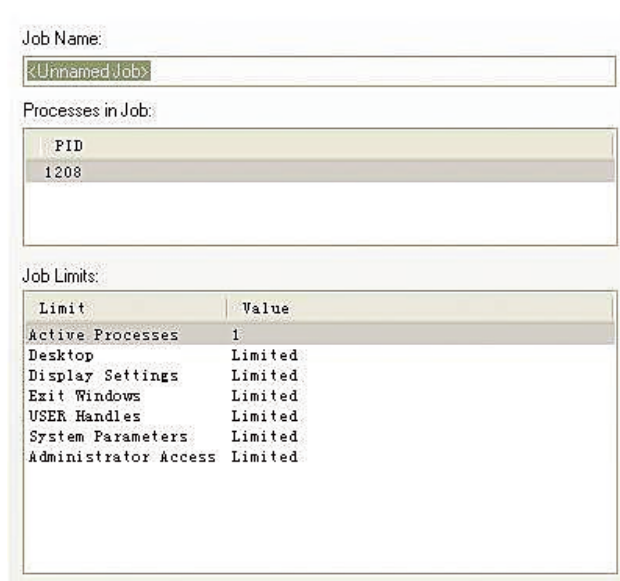


图 4 Adobe Reader X 作业对象

求的命令。测试 Adobe Reader X 打开记事本的命令，发现打开操作由代理进程完成。

Process Name	PID	Parent Process
AcroRd32.exe	440	Adobe Reader
AcroRd32.exe	1208	Adobe Reader
notepad.exe	1144	记事本

图 5 启动 Notepad 命令

## 受限令牌

Windows 使用令牌对象来标识一个进程的安全环境。令牌对象包含了 `SID` 和特权等，其中 `SID` 代表了创建进程的用户的账户和工作组，特权说明了进程可以对系统进行的操作。当进程访问一个

受保护的對象或進行一些系統操作的時候，Windows 將通過一個算法來對比令牌和被訪問對象的 DACL，然後決定操作是否成功。受限令牌就是去除和限制了令牌中不必要的權限，避免惡意代碼對系統的損害。主要體現在以下三個方面：

- 將令牌中的 SID 標記為 Deny;
- 在 Restrict SID 列表中添加 SID;
- 去除令牌中的特權。

將 SID 標記為 Deny 主要應對這種情況。令牌中的 SID 授予用戶的訪問權限是疊加的關係，如果令牌 T 中包含 A、B 兩個工作組的 SID，那麼用戶則可以訪問隸屬 A 工作組或隸屬 B 工作組的文件。由於對象 DACL 中的 Access Deny ACE 具有更高的優先級，如果文件 F 中包含針對 A 工作組的 Access Deny ACE，則令牌 T 將無法訪問文件 F，如果簡單去掉令牌 T 中 A 工作組的 SID 將會導致用戶有可能具備訪問文件 F 的權限。將 SID 標記為 Deny 則不會出現這種情況。

當令牌中存在受限 SID 列表的時候，Windows 將會兩次校驗 DACL 以決定訪問

權限，第一次根據普通 SID 和 deny SID 遍歷對象的 DACL，第一次檢查通過後再根據受限列表中的 SID 遍歷對象的 DACL，只有兩次檢查都成功才授予用戶訪問權限。

去除令牌中的特權可以防止用戶對系統進行惡意操作，如調試其他進程或加載驅動，也可以防止用戶繞過 Windows 對 SID 的檢查。例如如果用戶沒有對文件的訪問權限，但是卻有 SeBackupPrivilege，則用戶還是可以讀取文件。

受限令牌的核心函數是 CreateRestrictedToken()，他對一個已有令牌做修改並得到一個新的令牌，然後將新創建的令牌作為參數調用 CreateProcessAsUser() 對子進程做限制，CreateRestrictedToken() 如下：

```
BOOL CreateRestrictedToken(
    HANDLE ExistingTokenHandle,
    DWORD Flags,
    DWORD DisableSidCount,
    // 將 SID 標記為 deny
    PSID_AND_ATTRIBUTES SidsToDisable,
    DWORD DeletePrivilegeCount,
```

```
// 刪除特權
    PLUID_AND_ATTRIBUTES PrivilegesToDelete,
    DWORD RestrictedSidCount,
    // 在受限列表中添加 SID
    PSID_AND_ATTRIBUTES SidsToRestrict,
    PHANDLE NewTokenHandle
Adobe Reader X 對令牌的具體修改包括：
    • 將 BUILTIN\Users, Everyone, User's Logon SID, NTAUTHORITY\INTERACTIVE 之外的 SID 標記為 DENY_ONLY;
    • 將 BUILTIN\Users, Everyone, User's Logon SID, NTAUTHORITY\RESTRICTED 添加到受限 SID 列表;
    • 除 SeChangeNotifyPrivilege 之外，去除所有特權;
    • 添加 low integrity level SID (Windows Vista 之後的系統)。
通過 Process Explorer 觀察沙盒進程的令牌如圖 6 所示。
```



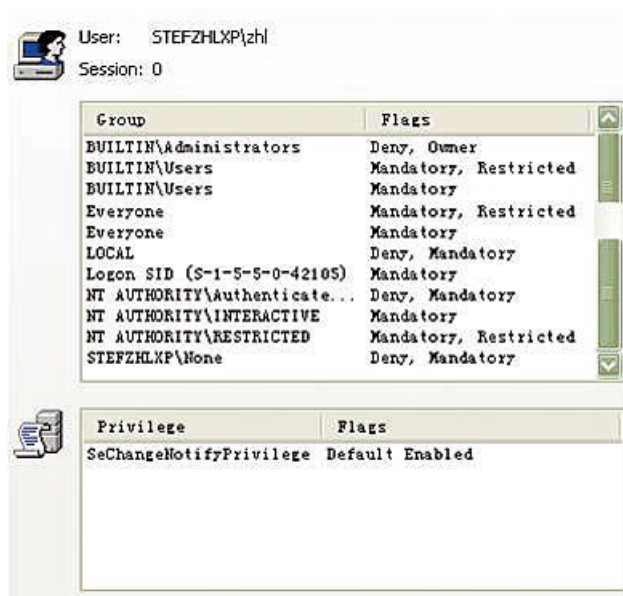


图 6 Adobe Reader X 令牌

显示结果和之前描述的相符。SeChangeNotifyPrivilege 没有被去除，因为许多系统调用依赖此特权。去除此特权将严重影响 Adobe Reader X 的功能。去除其它特权防止了恶意代码对系统进行破坏，也防止了恶意代码通过 CreateRemoteThread() 注入到其它进程来绕过沙盒保护。

Deny 和受限 SID 可以保证恶意代码无法进行以下操作：

- 释放文件到以下地方 (%windir%, C:\Documents and Settings, c:\Program Files, 磁盘根目录)；

- 修改、删除文件；

- 添加、修改、删除受保护的注册表键（包括自启动项）；

- 通过一些特权绕过沙盒，如调试其它进程，注入其它进程，加载驱动，备份文件等。

但是 Windows XP 没有限制向系统盘以外的磁盘子目录释放可执行文件，也没有限制读取用户文件，所以仍存在信息泄露问题。Windows Vista 后的系统，通过 UIPI 将沙盒进程设置为 Low integrity 级别，限制了向文件系统释放文件的行为。

### 隔离桌面

由于 Windows 设计的原因，在同一桌面下运行的程序存在如下安全问题：

- Shatter Attack
- SetWindowsHookEx
- Keylog
- 截屏

由于 Windows 允许同一桌面下的无特权的程序向高特权的程序发送消息，这将存在安全隐患。shatter attacks 是通过向其它进程发送消息来实现注入代码，一些 Windows 消息允许携带回调函数参数，如果攻击者可以通过某些方式向高权限进程写入 Shellcode，然后发送 WM\_TIMER 消息就可以实现在高权限进程执行代码。

在同一桌面下还可以通过 SetWindowsHookEx() 来向其它进程注入代码。Windows 程序还可以通过 GetKeyState() 获取同一桌面下的其它进程的击键信息。

通过隔离桌面可以防止此类的攻击。首先创建一个桌面，然后

调用 `CreatePorcessAsUser()` 并设置 `STARTUPINFO` 参数为新桌面。然而 Adobe Reader 的工程师评估了使用隔离桌面的可能，发现使用隔离桌面会对软件架构做相当大的变动，经过考虑暂不使用隔离桌面并通过其它机制防止同一桌面下实现存在的安全问题。Adobe Reader X 通过以下方式缓解此类攻击：

- 通过 Job 的 `UILIMIT_HANDLES` 限制，防止沙盒进程得到句柄，防止了 Shatter Attack 的攻击；
- 通过受限令牌去除特权，防止了通过 `SetWindowsHookEx()` 注入代码；
- 通过 UIPI 设置沙盒进程为 Low integrity 级别来防止 Shatter Attack、`SetWindowsHookEx()` 注入代码和 `KeyLog` (需要 Windows Vista 后的系统)。

目前在 Windows XP 下，还不能对

```
[> 我的电脑 <] (2011/28/04 - 10:24)
xcvxcvxcv

[> 我的文档 <] (2011/28/04 - 10:24)
11123456789
|
```

图 7 Windows XP 下进行键盘记录

`Keylog` 进行限制。如图 7。目前也无法对截屏进行限制。

### UAC

Windows Vista 操作系统开始支持 UAC, UIPI (User Interface Privilege Isolation, 用户界面权限隔离) 是 UAC 机制中的一部分。UIPI 将进程分为不同的 integrity 级别，从而保证低 integrity 级别的进程无法影响高 integrity 级别的进程。进程的 integrity 级别由令牌中的 SID 声明，系统预置了以下几个 integrity 级别：

此外还可以通过在令牌中设置 `S-1-16-xxxx` 来自定义 integrity 级别。UIPI 的基本原则是 no-write-up。Windows Vista 系统中每个受保护的對象都有一个 integrity 级别，系统首先进行 integrity 检查，然后再进

行原来的 DACL 检查。如果进程的 integrity 级别为 Low，而文件的 integrity 级别为 Medium，则进程无法写入文件。UIPI 具体所做的保护包括：

- 低权限级别进程无法对高权限级别的窗口句柄做验证，即无法判断窗口句柄是否有效；
- 低权限级别进程无法向高权限级别进程的窗口发送消息 (`SendMessage` 或 `PostMessage` 等等 API)。如果低权限级别进程向高权限级别进程的窗口发送了消息，使用的 API 将返回成功，而发送的消息会被丢弃；
- 低权限级别进程无法把线程注入到高权限级别进程；
- 低权限级别进程无法对高权限级别进

值	描述	符号
S-1-16-0000	不信任 (Untrusted level)	SECURITY_MANDATORY_UNTRUSTED_RID
S-1-16-4096	低 (Low integrity level)	SECURITY_MANDATORY_LOW_RID
S-1-16-8192	中 (Medium integrity level)	SECURITY_MANDATORY_MEDIUM_RID
S-1-16-12288	高 (High integrity level)	SECURITY_MANDATORY_HIGH_RID
S-1-16-16384	系统 (System integrity level)	SECURITY_MANDATORY_SYSTEM_RID

表 1 系统预置的 integrity 级别

程进行日志 (Journal) hook;

- 低权限级别进程无法把 DLL 注入到高权限级别进程。对窗口消息 hook 也就被隔离了;

- 低 integrity 级别的进程不可以读高 integrity 级别的地址空间。

还有一些系统资源是不受 UIPI 影响的, 也就是真正的全局共享的, 具体对象如下:

- 桌面窗口;
- 桌面堆 (Desktop heap)、只读的共享内存;
- 全局原子表 (Global atom table);
- 剪贴板。

默认情况下, 普通进程运行于 Medium integrity 级别, 文件系统中的文件默认是 Medium integrity 级别。而 Adobe Reader X 沙盒进程运行于 Low integrity 级别。所以 Adobe Reader X 的沙盒进程在 Windows Vista 以后的系统在被恶意攻击后也无法向用户系统释放文件。此外通过 UIPI 还可以防止 Shatter Attack、SeWindowHookEx()、Keylog 攻击。

### DEPPermanent

此外 Adobe Reader X 在系统开启 DEP 的情况下会设置 Adobe Reader X 进程的 DEP 状态为 DEPPermanent。设置为此状态后将无法在用户台再次关闭 DEP。恶意代码只能通过 ROP 等方式绕过 DEP。但是如果系统配置为不打开 DEP, 则 Adobe Reader X 无法使用 DEP 保护。

### 网络功能不受限制

虽然 Adobe Reader X 使用了作业、受限令牌、UAC 等机制限制沙盒进程的执行环境, 但是对于网络功能却没有任何限制。用户在受到攻击后, 恶意代码可以通过网络功能传送窃取到的数据。

### Hook API

由于 Adobe Reader X 沙盒的保护, 使得一些系统调用在沙盒进程中无法完成, 需要借助代理进程才能完成。Adobe 采用了 Hook API 的方式并在 hook 代码中利用 IPC 通讯请求代理进程完成需要的操作。通过测试发现被 hook 的 API 包括文件操作、注册表操作、进程操作、剪贴板操作等相关的 API。

### 漏洞利用对比

Adobe Reader X 的沙盒技术并不能阻止漏洞的产生, 只是在漏洞被触发后提高了漏洞利用的成本。下面来做一下 Adobe Reader

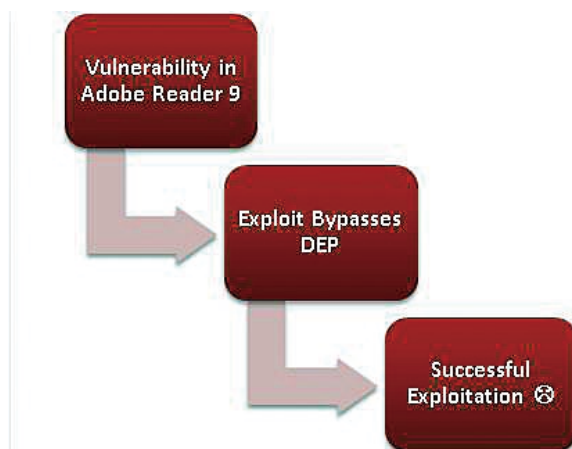


图 8 Adobe Reader 9+Windows XP 下漏洞利用

9 + Windows XP 和 Adobe Reader X + Windows 7 两个环境下漏洞利用的对比。

Windows XP 下 Adobe Reader 9 的进程运行在管理员权限下, 在触发漏洞后只需要绕过 DEP 就可以成功利用漏洞, 执行任意操作。

Windows 7 下首先需要触发 Adobe Reader X 沙盒进程的漏洞, 然后需要绕过 DEP, ASLP, SEHOP 等保护机制, 才能执行任意指令。但是由于沙盒进程运行于 Low integrity 级别, 这时还不能执行任意操作, 需要再次触发代理进程的漏洞, 然后再次绕过 DEP, ASLP, SEHOP 等保护机制才能得到正常用户的权限。由于 Windows 7 UAC 的保护, 代理进程不具备管理员权限, 所以还需要继续本地提

权才能对系统执行任意操作。

### 结论

Adobe Reader X 的沙盒主要依赖 Windows 系统的安全机制, 在一定程度上保护了用户系统的安全, 提高了漏洞利用的成本。目前, 沙盒可以防止恶意代码向系统安装程序, 但是恶意代码还是可以直接在 Adobe Reader 进程空间驻留, 并通过网络传送窃取到的数据。

### 参考资料

Inside Adobe Reader Protect Mode – Part 1 - Design

Inside Adobe Reader Protected Mode – Part 2 – The Sandbox Process

Inside Adobe Reader Protected Mode – Part 3 – Broker Process, Policies, and Inter-Process Communication

Inside Adobe Reader Protected Mode – Part 4 – The Challenge of Sandboxing

Practical Windows Sandboxing

[http://en.wikipedia.org/wiki/Shatter\\_attack](http://en.wikipedia.org/wiki/Shatter_attack)

Windows 核心编程

Windows Internals

Writing Secure Code 2nd edition

Writing Secure Code for Windows Vista

Escaping IE Protect Mode

Windows Vista UAC 研究

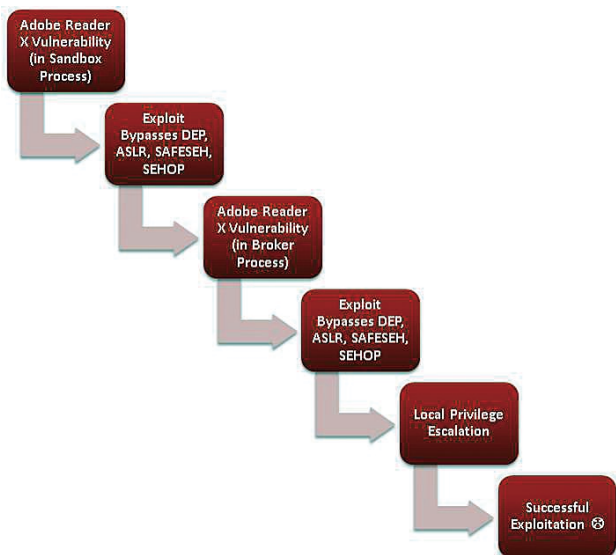


图 9 Adobe Reader X+Windows 7 下漏洞利用


# 图像识别在钓鱼检测中的应用

研发三部 张鸿勋

**摘要：**网络钓鱼攻击（phishing，又称钓鱼攻击、网络钓鱼）是一种近期高发的网络安全威胁。本文介绍了一种基于图像识别技术的网站徽标（LOGO）检测的新思路，用于过滤海量的疑似钓鱼页面。初步的实验表明了本文思路的有效性。

**关键词：**网络钓鱼 钓鱼检测 图像识别的应用 phishing Haar-like 特征 AdaBoost opencv

## 引言

 网络钓鱼是指一种企图通过伪造真实的网页来欺骗使用者，从而获取使用者的银行账号、密码等个人敏感信息的犯罪诈骗过程。近期，网络钓鱼事件频繁发生，2011年初中国银行发生的钓鱼事件，更是引起了业内外广泛的关注<sup>[1]</sup>。

本文提出了一种基于网站徽标（LOGO）识别的钓鱼网页过滤新思路，通过检测网页中是否包含相关机构和组织的 LOGO 图标，来加速海量疑似钓鱼网页的监控和判定流程。本文组织如下：第一章主要介绍钓鱼检测和图像识别的相关内容，第二章介绍了 LOGO 识别原理、实验过程和结果分析，最后给出了结论和后续工作的方向。

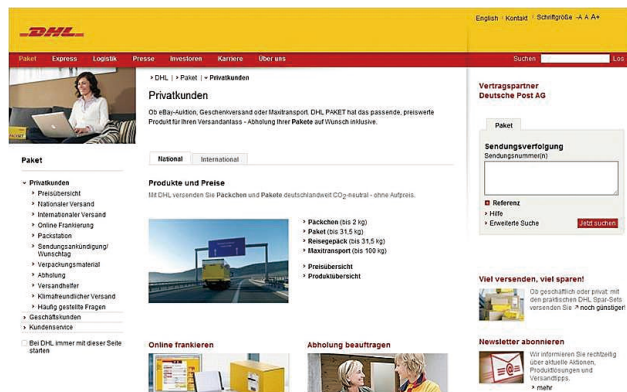
## 1、钓鱼检测和图像识别简介

钓鱼攻击的检测可以理解为在大量的可疑的网页中，找到和被保护的网页“相似的”的页面的过程。业内对这种“相似页面”的钓鱼检测的思路主要有以下几种：一是判定网页结构、内容的相似度，二是将网页看作图片，比较两个图片的相似度，以及将上面两种方法进行一定的融合<sup>[2]</sup>。

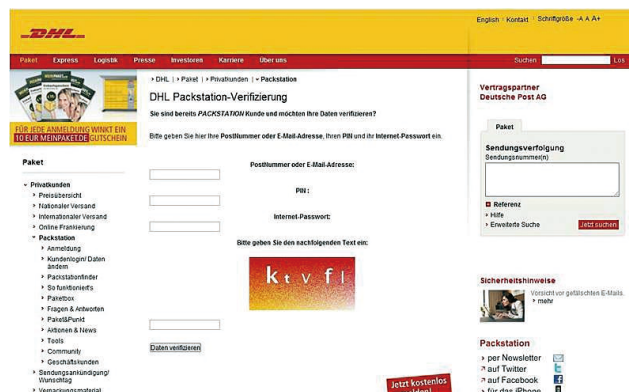
攻击者要想钓鱼攻击成功，其制作的伪造页面一定要在视觉上

和原始页面很像，这样才能很大程度上提高钓鱼的成功率。我们也注意到大部分的被钓鱼的组织或者机构（银行、航空公司等）的官方网站都会包含相应的组织徽标 LOGO，由于伪造页面和原始页面十分相似，因此在很大程度上伪造的页面也会包含相应的 LOGO。图 1 是某公司德文官方页面和相应的钓鱼页面的对比图，数据来自 PhishTank<sup>[3]</sup>。从图中可以看出，钓鱼页面和被保护的页面非常相似，且都含有官方的 LOGO。

正是基于此点原因，如果能够应用图像识别技术，在海量的网



a. 某公司德文官方网站页面



b. 某钓鱼页面

图 1 某公司德文官方网站和相应的钓鱼网站

页中迅速的筛选出包含有特定 LOGO 的网页，必将大大的提升发现钓鱼站点的效率。

图像识别是人工智能和机器学习的一个重要且成熟的研究领域。

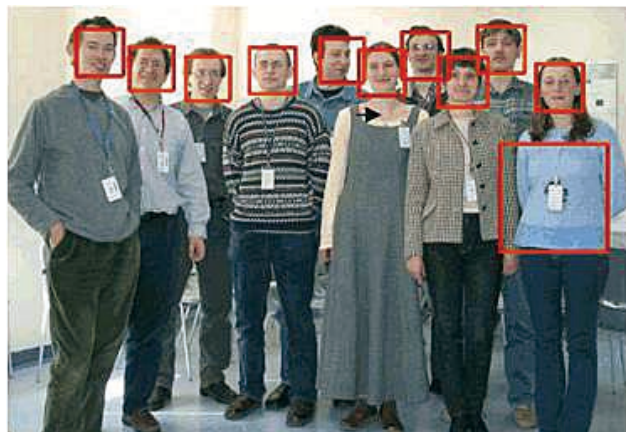


图 2 人脸识别示例

在工业中有广泛的应用，比如人脸识别，车牌检测和验证码的识别等领域<sup>[4]</sup>。图 2 是一张来自于 opencv 网站的图片，通过训练分类器，可以在图片中标识出人脸的位置。

在一张图片中识别出人脸和在一张网页的截图中识别出 LOGO，实际上是等价的。都可以看作是一种分类问题，因为在检测的过程中，算法会根据检查窗口的大小进行截图，来判断这个截图是否为特定的类别（人脸或者 LOGO）。

## 2. 基于 Haar-like 特征的 LOGO 识别和分析

分类问题是机器学习领域的一个经典问题，是监督学习的一种。顾名思义，分类器主要是在给定训练数据然后进行相应的特征抽取后，训练出一个数学模型，这个模型可以对后续的数据进行分类。那么，我们的目标就是构建一个 LOGO 识别的分类器，其中有两个关键的步骤：一是特征抽取，用一组特征来表示原始数据图片。二是用特征抽取后的正负例来训练分类器，使其具有分类能力，下面主要从这两个方面来介绍。

### 2.1 图片特征抽取和 Haar-like 特征

特征抽取的目的是为了在不损失太多信息的情况下，来提高分类器的计算速度。理论上，可以直接用图片的每个像素作为一个特征来直接分类，但是这会带来巨大的计算量，同时由于特征向量的维数太高，通常分类效果不是很理想。因此，Viola and Jones 借鉴 Haar 小波变换的思想，于 2001 年提出了 Haar-like（以下简称 Haar）的特征抽取的方法<sup>[5]</sup>，从而极大的提高了特征抽取的速度。

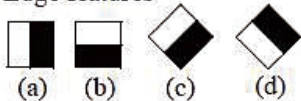
Haar 特征的类型主要分为边特征、线特征以及中心环绕特征等

## ▶▶ 前沿技术

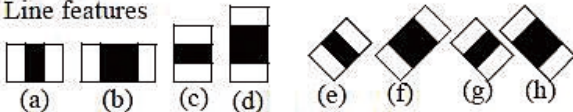
类型。特征抽取主要方法是通过计算每个像素的积分图，来匹配图 3-a 中的这些特征的过程。最后使用一组特征的组合来表示一个图片。

Haar 特征最大的优势在于计算速度，由于使用了积分图，对于任意大小的图片来说，都可以在恒定的时间内计算完毕。将训练数据

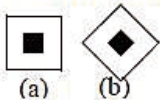
## 1. Edge features



## 2. Line features



## 3. Center-surround features



a. 各种类型的 Haar 特征



b. Haar 特征匹配图示

图 3 Haar 特征及其匹配过程举例



a. 正例 (positive samples)



b. 一个负例图片 (negative sample)

图 4 用于 LOGO 识别的正例和负例

进行了 haar 特征化之后，就可以作为分类器的输入数据进行训练了。

对于 LOGO 识别问题来说，我们主要需要准备两类数据，我们称其为正例样本 (positive samples) 和负例样本 (negative samples)。其中正例样本包括的都是我们要识别的 LOGO 图片，负例样本是指不包括的待识别的 LOGO 的图片。图 4 所示的是部分的正例和负例样本截图。有了这两类数据，我们就可以进行分类器的训练了。

## 2.2. 分类器和 AdaBoost 介绍

在具体的介绍实验之前，我们先来了解一下分类器的相关知识。

用于图片识别的分类器算法和模型有很多，比如人工神经网络 (Artificial Neural Network, ANN)，支持向量机 (Support Vector Machine, SVM)，以及 AdaBoost (Adaptive Boosting) 等，其中 AdaBoost 分类器在速度和精度上最好，下面简单介绍一下 AdaBoost 分类器。

AdaBoost 分类器算法于 1995 年由 Freund 和 Schapire 提出<sup>[6]</sup>，该算法主要是将弱分类算法提升为强分类算法的一种算法。所谓弱分类算法是指分类准确率仅高于 50% 的算法，也就是仅仅比随机分类算法略强，强学习算法是指分类准确率较高的分类器算法。AdaBoost 的神奇之处就是通过将若干弱分类器进行线性组合，然后根据每个分类器的权重、投票，来将整体的分类准确率大大提高。其算法流程<sup>[7]</sup>如下：

1. 初始化训练数据及其权重
2. 训练弱分类器：
  - a) 根据每个特征训练 T 个弱分类器
  - b) 从 T 个弱分类器中选出错误率最低的分类器 T-best
  - c) 根据 T-best 调整其他弱分类器的权重
3. 生成强分类器（弱分类器的线性组合）

AdaBoost 更加详细的介绍、原理和证明过程不在本文的讨论范围之内，具体请参见 PAC 学习理论<sup>[8]</sup>。

### 2.3. 实验和分析

我们采用了 opencv2.2 进行相应的实验。训练数据是通过绿盟

科技钓鱼监控服务平台产生，正例为东航网站 LOGO，共 300 张，负例为不包括东航 LOGO 的 1000 张随机网站截图。具体的训练流程如下：

#### 1. 创建正例数据：

```
opencv-createsamples -vec pos.vec -info pos/pos.txt -bg neg/neg.txt -w 20 -h 20 -num 300
```

#### 2. 训练分类器：

```
opencv-haartraining -data logo -vec pos.vec -bg neg/neg.txt -npos 300 -nneg 1000 -w 20 -h 20 -mem 800 -mode all -nonsym -minhitrate 0.995 -maxfalsealarm 0.5
```

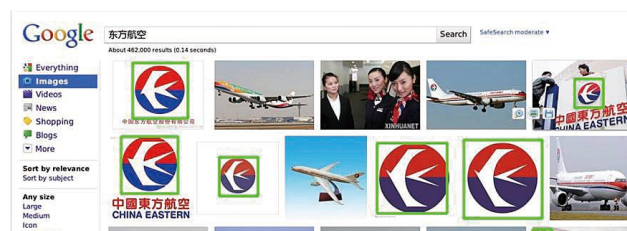
其中，opencv-createsamples 是 opencv 开发包提供的打包正例图片的程序。opencv-haartraining 是 opencv 开发包提供的分类器训练程序。具体的训练参数说明，请参看 opencv 相关说明文档。

```
def detect(srcfile):
    try:
        image = cv.LoadImage(srcfile, 1)
    except:
        return None, 0
    image_size = cv.GetSize(image)
    grayscale = cv.CreateImage(image_size, 8, 1)
    cv.CvtColor(image, grayscale, cv.CV_BGR2GRAY)
    cv.EqualizeHist(grayscale, grayscale)

    # detect objects
    cascade = cv.Load('logo.xml')
    mem = cv.CreateMemStorage(0)
    logos = cv.HaarDetectObjects(grayscale,
        cascade,
        mem, 1.2, 2,
        cv.CV_HAAR_DO_CANNY_PRUNING,
        (20, 20))
    for (x, y, w, h), n in faces:
        cv.Rectangle(image, (x, y), (x+w, y+h), (0, 255, 0), 4)
    return image, n
```

图 5 LOGO 识别代码片段 (python)





a LOGO 识别结果图



b LOGO 识别误报举例

图 6 LOGO 识别结果示例

训练成功后，生成分类器的模型文件 logo.xml，我们就可以在应用中使用此分类器进行 LOGO 识别了，python 脚本片段如图 5 所示。

如图 6 所示，初步的实验结果表明，在上面给出的数据集和参数设置下，分类器的漏报率 (False negative rate) 很低。换句话说，只要图片中包含东航的 LOGO，基本上都能够被分类器识别出来。但是，问题主要集中在误报率 (False positive rate) 较高上，就是说在一张没有 LOGO 的图片上，分类器却识别出来 LOGO 发生了误报。根据分类器的原理分析可知，对于此类问题可以通过增加负例的样本量，让分类器在训练的过程中“见识”到更多的负例样本，来进一步降低误报率，这也是下一步实验的主要方向之一。

### 3、总结和下一步工作展望

本文介绍了钓鱼网络攻击以及图像识别技术在钓鱼检测过程中的应用，提出了一种通过基于网站徽标 LOGO 识别来过滤海量钓鱼页面的新思路，初步的实验证明了思路的有效性。

另外对于 LOGO 识别来说，分类器的漏报率是相对较低的，但是误报率却较高。分析表明可以通过增加负例样本的样本量来改进此问题，这也是下一步实验的主要方向。

#### 参考资料：

- [1]. 凤凰网，中国银行用户被钓鱼 网银安全遭质疑 \_ 财经 \_ 凤凰网，<http://finance.ifeng.com/bank/special/zhongguooyinhjm/index.shtml>, 2011
- [2].Fu, A.Y., Detecting Phishing Web Pages with Visual Similarity Assessment Based on Earth Mover's Distance(EMD), X.D. Liu Wenyin, X.D. Liu Wenyin^Editors. 2006. p. 301-311.
- [3]. 反钓鱼网站，<http://www.phishtank.com>
- [4]. 新华网，我国研制的人脸识别技术成功用于奥运会，[http://news.xinhuanet.com/tech/2008-08/30/content\\_9738626.htm](http://news.xinhuanet.com/tech/2008-08/30/content_9738626.htm)
- [5].P., V., Rapid object detection using boosted cascade of simple features, J.M. J., J.M. J.^Editors. 2001. p. 8-14.
- [6].Y., F., Boosting a Weak Learning Algorithm by Majority, Information and Computation, 1995. 第 256-285 页。
- [7].J., V.P.J.M., Robust Real-Time Face Detection. 2004. p. 137-154.
- [8].G., V.L., A Theory of the Learnable, Communications of the ACM, 1984. 第 1134-1142 页。

### 绿盟科技 WEB 应用防火墙占据中国区市场份额首位

近日，国际权威咨询机构 Frost & Sullivan 发布了《Asia Pacific (including Japan) Web Application Firewall Market CY2010》(2010 年亚太地区 WEB 应用防火墙市场报告)。报告指出，绿盟科技 WEB 应用防火墙（以下简称 WAF）以 25.2% 占有率位列中国区市场份额首位。

这是国际权威咨询机构首次发布详细的 WAF 市场份额报告。此份市场报告也反映出随着 WEB 应用威胁的发展，WAF 已经开始从新概念产品发展成为一类主流安全产品，进入了国际权威咨询机构的分析视野。

自 2008 年 1 月发布国内首款 WEB 应用防火墙，绿盟科技 WAF 产品通过 3 年多的持续研发，功能不断创新，稳定性不断提高，正是基于这些深厚扎实的积累，绿盟科技 WAF 才获得了众多用户的选择与信赖。截止目前，已经服务于运营商、金融、政府等各个行业的 400 多家客户。在未来，绿盟科技还将在安全功能和服务模式上持续创新发展，源源不断地把自己对 WEB 安全漏

洞、威胁的理解和防护能力提供给客户，包括借助“云服务”生成的虚拟补丁等，为客户提供更加全面的 WEB 安全保障方案。

### 绿盟科技反钓鱼网站监控服务上市

近期，网络钓鱼攻击频繁发生，多家金融机构受到牵连。如何及时、有效地识别网络钓鱼相关的互联网风险，控制钓鱼攻击可能带来的影响，已经成为各金融机构当前亟待解决的问题。正是在这一背景下，绿盟科技推出了反钓鱼网站监控解决方案。旨在根据监管要求，协助用户及时发现已存在的相关钓鱼网站，以及可能被钓鱼攻击利用的弱点，并有效控制钓鱼网站的影响范围，从而减少钓鱼攻击可能带来的损失。

作为一种主要基于互联网传播和实施的新兴攻击、诈骗的方式，“钓鱼攻击”(Phishing Attack) 正呈逐年上升之势，这一方面致使广大用户遭受到财产和经济损失，另一方面也让金融证券机构、电子商务公司的声誉和形象受到了极大影响。“钓鱼不再只是个人人的小打小闹，而是有组织、有分工，有技术支持、有自己独特盈利模式的群体诈骗活动，给社会造成了极大的危害”，根据中国反

钓鱼网站联盟 (APAC) 发布的数据显示，“仅 2011 年 4 月份一个月联盟处理的钓鱼网站数量就达到 2635 个”。钓鱼攻击的危害不言而喻，但是由于钓鱼站点传播方式的多样性以及钓鱼站点本身的伪装性，发现钓鱼站点目前多数还依靠网银用户投诉的方式，同时发现钓鱼站点后，也缺乏有效的手段对钓鱼站点的传播进行控制。

绿盟科技反钓鱼网站监控服务，基于绿盟科技云安全平台，主动进行大范围互联网仿真站点的检索。每天千万级页面的处理能力，数十万种域名变形的搜索算法，同时结合针对被保护站点的定期脆弱性评估、7\*24 小时安全状态监测，从而确保能及时发现和用户相关的钓鱼网站。一旦发现并确认钓鱼站点后，绿盟科技将协助用户进行应急响应。一方面，向主管机构上报，协调关闭钓鱼网站；另一方面，向合作伙伴提交信息，从客户端及时阻断恶意网站的访问请求，以控制此类攻击的影响范围。

作为中国反钓鱼网站联盟成员单位，积极参与反钓鱼技术研讨，希望为广大成员单位，乃至更多的金融、电子商务、互联网公

司提供更多的专业服务。历经多年的不间断安全研究及技术创新，绿盟科技在脆弱性评估与安全管理这一领域积累了丰富的实践经验，针对 Web 应用，形成了从“漏洞扫描”、“配置管理”、“威胁防护”到“实时监测”，全方位的 Web 应用安全解决方案布局，为客户提供从产品到服务多种安全交付能力，最终全方位保障客户的网站安全。

### 绿盟科技持续领跑国内入侵防御硬件市场

近日，国际权威咨询机构 IDC 发布了《中国 IT 安全硬件、软件和服务全景图，2011-2015》报告。报告显示，绿盟科技网络入侵防护系统（以下简称 NIPS）以 17.5% 占有率位列中国入侵防御硬件市场第一名。

根据 IDC 报告的统计数据 displays，2010 年中国 IT 安全硬件市场增速放缓，全年整体仅实现 8% 的增长。其中，入侵防御硬件市场的表现低于预期，与 2009 年同比仅增长 6.1%，远低于 2010 年上半年报告中预测的 31.3%。这也直接导致入侵防御市场的竞争相当激烈，市场排名也再次发生了变化。绿盟科技 NIPS 凭借可靠的品质和领先的技术赢得用户的信赖，以远高于市场平均增速

的高增长率，持续领跑国内入侵防御硬件市场。

作为漏洞分析和攻防研究领域的领导厂商，绿盟科技时刻关注各类安全威胁变化，并持续提升产品和服务品质。经过多年的潜心研究与发展，绿盟科技 NIPS 在 2010 年 3 月顺利通过 NSS Labs 严格测试，并获得国内首个、全球第四个“Recommended”高级别认证，能够为用户提供具有国际品质的高性价比入侵防护解决方案。

### 绿盟科技网站安全监测系统上市

日前，绿盟科技基于多年对 Web 应用安全的研究与积累，推出了专用于网站安全风险监测的产品——绿盟网站安全监测系统（简称：NSFOCUS WSM），旨在根据网站系统监管要求，通过对目标站点进行页面爬取和分析，为用户提供透明模式的远程集中化安全监测、风险检查和安全事件的实时告警，并为客户提供全局视图的风险度量报告，最终帮助客户构建完善的网站安全体系。

随着 Web 应用的日益广泛及其蕴藏价值的不断提升，引发了越来越多的攻击热潮。根据国家互联网应急中心（CNCERT/CC）

2011 年发布的《中国互联网安全报告》显示，2010 年中国大陆有近 3.5 万个网站被黑客篡改，其中被篡改的政府网站高达 4635 个，比 2009 年上升 67.6%。日益严重的 Web 应用安全问题给传统应用安全评估方式带来了挑战。传统安全评估工作中所采用 Web 应用漏洞扫描工具在扫描规模、页面爬取和分析能力、检测结果关联分析等方面存在局限性，并且无法做到高频率的风险监测、及时发现风险，因此需要有专门针对 Web 应用安全的监测系统对网站进行安全监管。

新上市的绿盟网站安全监测系统能够多维度、高频率地洞察站点群的各项风险隐患，可对目标站点进行全方位的风险监测，一旦发生高危安全事件，能够及时告警，第一时间帮助客户降低风险。该产品采用了远程透明监测技术，无需改变现有网站结构，只要对 NSFOCUS WSM 系统进行简单配置，无需部署任何代理设备，就可对用户网站远程监测；并且可以提供可视化、全局视图的风险度量报告，展示各级站点整体风险状况。

# NSFOCUS 2011年7月之十大安全漏洞

**声明：**本十大安全漏洞由 NSFOCUS( 绿盟科技 ) 安全小组 > 根据安全漏洞的严重程度、利用难易程度、影响范围等因素综合评出，仅供参考。[http://www.nsfocus.net/index.php?act=sec\\_bug&do=top\\_ten](http://www.nsfocus.net/index.php?act=sec_bug&do=top_ten)

---

## 1. 2011-07-04 Apple iOS Postscript Type 字体处理缓冲区溢出漏洞

---

NSFOCUS ID: 17178

<http://www.nsfocus.net/vulndb/17178>

综述：

Apple iOS 是苹果公司推出的操作系统。

Apple iOS 在处理 Postscript Type 字体时存在漏洞，漏洞存在于 t1\_decoder\_parse\_charstrings() 函数，可以导致执行任意代码。此漏洞已经被用于苹果系统的越狱。

危害：

远程攻击者可以利用此漏洞，诱使受害者打开恶意的 Type1 字体，从而控制受害者系统。

---

## 2. 2011-07-08 FreeType PostScript Type1 字体解析漏洞

---

NSFOCUS ID: 17187

<http://www.nsfocus.net/vulndb/17187>

综述：

FreeType 是一个用 C 语言实现的字体光栅化引擎制作的一个库。

FreeType 在实现上传存在字体解析漏洞，远程攻击者可利用此漏洞控制用户系统。

危害：

远程攻击者可以利用此漏洞，诱使受害者打开恶意的 Type1 字体，从而控制受害者系统。

## ▶▶ 安全公告

### 3. 2011-07-20 Cisco SA 500 系统设备 Web 管理界面远程命令注入漏洞

NSFOCUS ID: 17312

<http://www.nsfocus.net/vulndb/17312>

#### 综述：

Cisco SA 500 系列安全设备是集成的安全解决方案，针对不到 100 个员工的小型企业。

Cisco SA 500 系列产品在 Web 管理界面的实现上存在远程命令注入漏洞。

#### 危害：

远程攻击者可以利用此漏洞，在 Web 表单中提供恶意参数，以 root 权限在下层操作系统中执行任意命令。

### 4. 2011-07-13 Trend Micro Control Manager "module" 参数目录遍历漏洞

NSFOCUS ID: 17226

<http://www.nsfocus.net/vulndb/17226>

#### 综述：

Trend Micro Control Manager 是一款安全解决方案。

Trend Micro Control Manager 在 module 参数的实现上存在目录遍历漏洞。TMCM 在用于读取文件之前，没有正确验证通过 "module" 参数发送到 WebApp/widget/proxy\_request.php 的输入，导致了目录遍历问题。

#### 危害：

远程攻击者可利用此漏洞获取服务器上的任意文件。

### 5. Windows Bluetooth 栈 bthport.sys 驱动程序远程代码执行漏洞 (MS11-053)

NSFOCUS ID: 17198

<http://www.nsfocus.net/vulndb/17198>

#### 综述：

Microsoft Windows Bluetooth stack 是蓝牙协议栈的实现。

Microsoft Windows Bluetooth stack 未能正确初始化或处理已被删除内存对象，存在远程代码执行漏洞。

#### 危害：

远程攻击者可利用此漏洞，发送特制的蓝牙报文到受影响系统，导致远程代码执行。

### 6. phpMyAdmin 多个安全漏洞

NSFOCUS ID: 17174

<http://www.nsfocus.net/vulndb/17174>

#### 综述：

phpMyAdmin 是用 PHP 编写的工具，用于通过 WEB 管理 MySQL。

phpMyAdmin 在实现上存在多个漏洞，包括执行 PHP 命令，目录遍历等。

**危害：**

远程攻击者可以利用此漏洞，向服务器提交恶意的 HTTP 请求，对服务器进行非授权的访问。

---

**7. 2011-07-19 Oracle Database Server 远 程 Core RDBMS 漏洞 (CVE-2011-2253)**

---

NSFOCUS ID: 17260

<http://www.nsfocus.net/vulndb/17260>**综述：**

Oracle Server 是一个对象—关系数据库管理系统。

Oracle Database Server 在实现上存在远程 Core RDBMS 漏洞。

**危害：**

远程攻击者可利用此漏洞，通过 Oracle NET 协议，对数据库进行非授权的访问。

---

**8. 2011-07-19 Oracle Database Server RDBMS 远 程 Core RDBMS 漏洞 (CVE-2011-2239)**

---

NSFOCUS ID: 17259

<http://www.nsfocus.net/vulndb/17259>**综述：**

Oracle Server 是一个对象—关系数据库管理系统。

Oracle Database Server 在实现上存在远程 Core RDBMS 漏洞。

**危害：**

远程攻击者可利用此漏洞，通过 Oracle NET 协议，对数据库进行非授权的访问。

---

**9. 2011-07-05 ISC BIND UPDATE 请求处理拒绝服务漏洞**

---

NSFOCUS ID: 17177

<http://www.nsfocus.net/vulndb/17177>**综述：**

BIND 是一个应用非常广泛的 DNS 协议的实现。

ISC BIND 在处理特制的 UPDATE 请求时存在拒绝服务漏洞，此漏洞源于处理 UPDATE 请求时的错误，特制的 UPDATE 请求将导致 named 进程中断。

**危害：**

攻击者可以利用此漏洞，向服务器发送特制的 UPDATE 请求，导致拒绝服务。

---

**10. 2011-07-07 Symantec Web Gateway Management GUI SQL 注入漏洞 (CVE-2011-0549)**

---

NSFOCUS ID: 17185

<http://www.nsfocus.net/vulndb/17185>**综述：**

Symantec Web Gateway 是赛门铁克企业级网页威胁防护解决方案。

Symantec Web Gateway 在 SQL 查询中直接使用用户提供的数据，通过 "username" 参数发送到管理界面的 forget.php 在用于 SQL 查询时没有正确过滤，导致了 SQL 注入。

**危害：**

远程攻击者可以利用此漏洞，向服务器提交恶意的 HTTP 请求，对数据库进行非授权的访问。

# 巨人背后的专家



- 2010年：绿盟科技入侵防御产品(NSFOCUS IPS)荣获NSS Labs最高级别认证
- 2009年：荣获Frost&Sullivan颁发的“2009年中国IDS/IPS市场增长战略领导者”奖
- 2008年：绿盟科技“极光”远程安全评估系统成为1996年以来全球六家获得英国西海岸实验室权威认证的漏洞扫描产品之一
- 2007年：再次入选国家级应急服务支撑单位
- 2006年：连续四年荣获中计报“值得信赖的安全服务品牌”
- 2005年：囊括年度入侵检测\保护系统全部奖项
- 2004年：入选公共互联网应急处理国家级服务试点单位首批荣获国家二级安全服务资质
- 2003年：进入中国电子政务IT百强
- 2002年：承担全国性电信网安全评估
- 2001年：入选国家网络安全服务试点单位
- 2000年：绿盟科技成立

[www.nsfocus.com](http://www.nsfocus.com)

## THE EXPERT BEHIND GIANTS

长期以来，绿盟科技致力于网络安全技术的研究，为政府、运营商、金融、能源等行业提供优质的安全产品与服务。在这些巨人的背后，他们是倍受信赖的专家。



NSFOCUS



THE EXPERT BEHIND GIANTS 巨人背后的专家