



面向企业网的 APT 攻击特征分析及防御技术探讨

刘东鑫, 刘国荣, 王 帅, 沈 军, 金华敏

(中国电信股份有限公司广东研究院 广州 510630)

摘 要:近年来, APT 攻击成为信息安全业界的关注热点。针对 APT 攻击特征分析传统网络安全防御体系对其失效的原因, 并在此基础上提出 APT 攻击防御方案。该防御方案包括基础安全防御和动态防御体系, 力求构建从保护、检测、响应到恢复的信息安全防御体系。最后, 对 APT 攻击给业界带来的影响进行了思考和展望。

关键词: APT; 特征分析; 动态防御

doi: 10.3969/j.issn.1000-0801.2013.12.026

Research on the Defense of Advanced Persistent Threats in Enterprise Network

Liu Dongxin, Liu Guorong, Wang Shuai, Shen Jun, Jin Huamin

(Guangdong Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China)

Abstract: Recently, advanced persistent threats have become a hot spot of information security industry as so many reports were taken about that some famous companies had been suffered from it. The features of APT and the reason why traditional security defense architecture was failed were discussed. After that, a solution was proposed to build a PDRR defense model. In the end, the impacts that APT brings in was discussed.

Key words: advanced persistent threat, feature analysis, dynamic defense

1 引言

APT(advanced persistent threat, 高级持续性威胁)中的“advanced”可理解为突破了现有的网络安全纵深防御体系;“persistent”可理解为在攻击目标组织内长期潜伏, 不被发现;“threat”可理解为有目的、有组织的恶意攻击行为。近年来, APT 攻击成为信息安全业界的热点话题, 众多大公司如 Google、RSA、Sony 等都先后公开承认遭受 APT 攻击, 造成机密数据泄露等一系列严重后果, 如图 1 所示。一系列 APT 攻击事件震惊业界, 越来越多的大型企业开始对其给予高度关注^[1]。

实践证明, 传统的安全防御手段难以有效应对 APT

攻击, 亟需新的安全防御思路和技术。因此, 本文将从几个著名的 APT 攻击案例出发, 分析其典型特征、与传统网络安全攻击方法的差异对比; 然后在分析传统网络安全防御手段失效原因的基础上, 提出 APT 攻击防御方案, 并对实施流程和关键技术作了说明和分析; 最后分析 APT 攻击给业界带来的长远影响。

2 APT 攻击特征及传统网络安全防御体系失效原因

2.1 全球著名 APT 攻击的案例分

(1) Google 遭受 Aurora 攻击

2010 年, 互联网的明星企业 Google 公开承认遭受

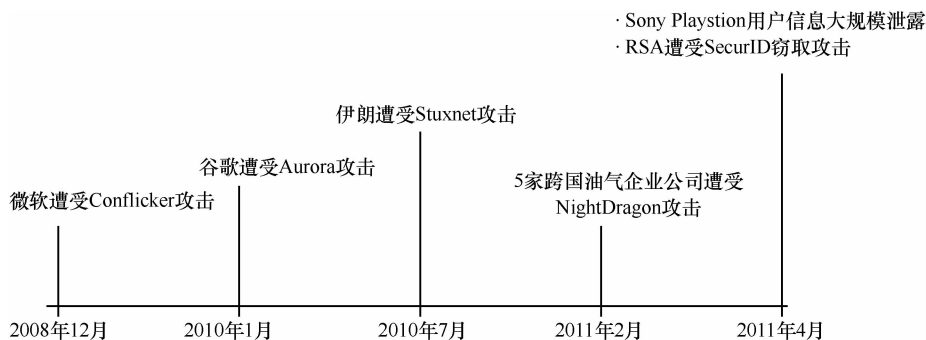


图1 近年来 APT 攻击重大事件

APT 攻击,造成关键数据泄露。这一事件后来被命名为 Aurora 攻击。事件过程是:一位员工点击了来自社交网络好友所发送即时消息中的一条恶意链接,随后造成 IE 浏览器溢出、自动下载恶意程序;随后,攻击者使用 SSL 安全隧道间歇性地控制该员工的主机,最终侦听到该员工访问 Gmail 服务器的账号信息。此次攻击造成包括系统管理员账号、Gmail 用户信息等一系列关键数据泄露,整个过程持续数月之久。这次攻击过程如图 2 所示。

(2)RSA 遭受 SecurID 窃取攻击

2011 年 3 月,信息安全业界的领军企业——RSA 公司遭受 APT 攻击,导致部分 SecurID 技术及客户资料泄漏。随后,很多使用 RSA 的 SecurID 作为认证凭据建立 VPN 的企业受到攻击,导致企业的重要资料文件被窃取。事件的过程是:攻击者直接寄送电子邮件给 RSA 公司的众多内部员工,并在 Excel 文件附件中利用最新的 0day 漏洞隐藏了恶意程序;某位内部员工在打开文件附件后,恶意程序在其主机自动运行,并被植入 Poison Ivy 远端控制工具;后续过程与 Aurora 攻击类似,其攻击过程如图 3 所示。

2.2 APT 攻击的特征总结

基于以上全球著名 APT 攻击案例分析,结合与传统网络攻击方法的对比,对其攻击特征进行进一步的分析总结。首先,从攻击目标来看,APT 攻击不以破坏目标系统的可用性、可靠性为主要目的,旨在窃取高价值的数据、资料、文件;其次,从攻击方法来看,APT 攻击者通常不计成本地挖掘、购买 0day 漏洞,甚至自行开发恶意软件以绕过现有的 IDS/IPS、反病毒软件系统,在此基础上进一步采用社会工程学方法在目标企业内部员工的电脑主机中建立攻击支点;最后,从防护技术来看,相较于传统网络攻击易于被现有安全防护设备检测、防范,APT 攻击的潜伏时间长,难以被已有的安全防护系统所检测,甚至在攻击后,也难以被溯源。更恶劣的是,如果攻击者所利用的脆弱性没有被及时修复,APT 攻击随时可能卷土重来,对企业网络的安全防御体系形成严峻的挑战。因此,面对 APT 攻击,企业的网络安全防御亟需新的思路 and 手段。

2.3 传统网络安全防御体系失效原因

时至今日,APT 攻击在全球成为信息安全业界挥之不去的阴霾,成为悬在众多著名 IT 企业甚至政府机构头顶

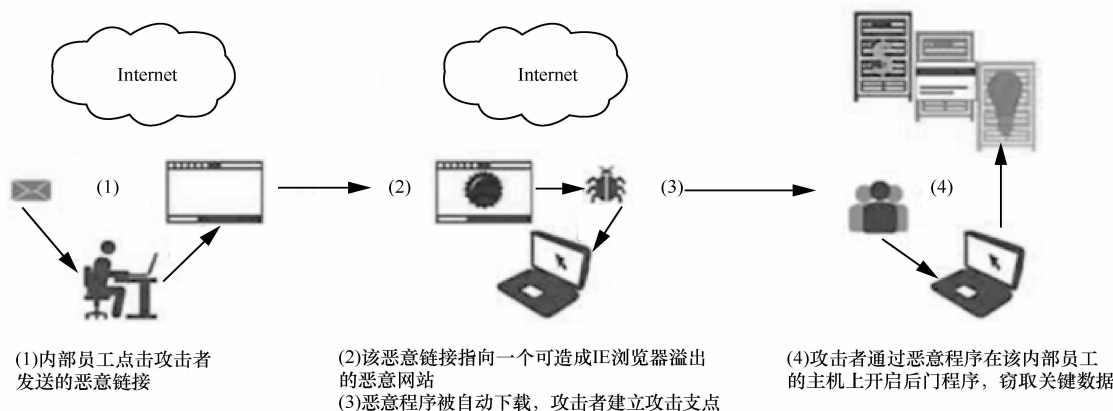


图2 Google 遭受 Aurora 攻击流程

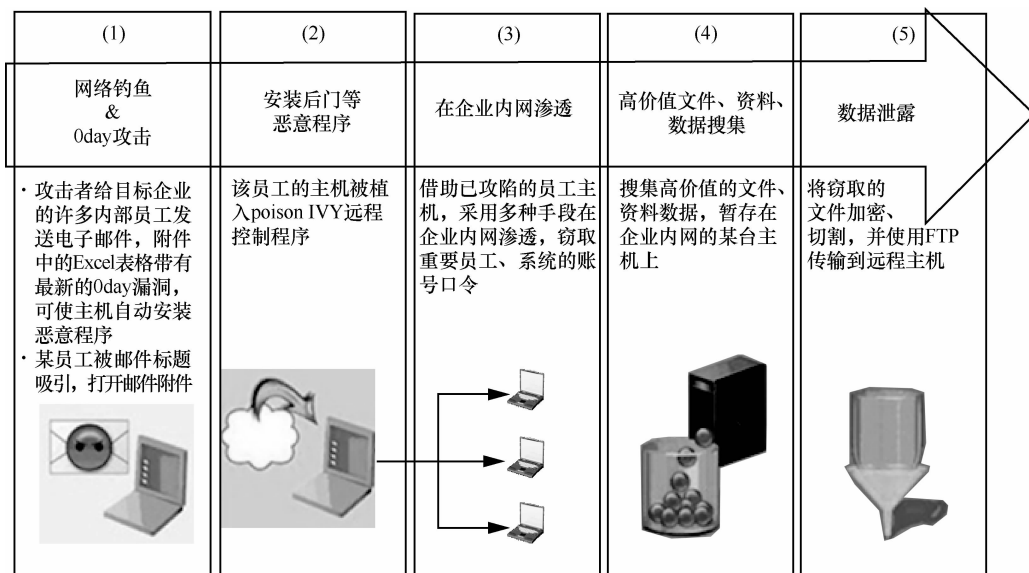


图3 RSA 遭受 SecurID 窃取攻击流程

的“达摩克利斯之剑”。从 APT 攻击的工具、手段和过程来看,目前传统网络安全防御体系的失效,在技术方面主要包含以下原因。

- 反病毒软件难以检测攻击者“独门”开发的恶意程序。理想状态下,反病毒软件应能实时检测出任何恶意代码,并阻止其运行。但是现有大部分反病毒软件仍然以特征码技术作为主要的病毒检测手段,一旦用户的计算机遇到最新病毒,在厂商发布针对该病毒的特征码之前,反病毒软件将难以检测出来。而 APT 攻击者往往利用常用软件的 Oday 漏洞,针对目标对象开发特有的恶意程序,致使市场上的反病毒软件无法对其进行有效检测。
- 防火墙设备难以检测应用层加密的网络流量。理想状态下,防火墙应能阻止或者限制任何未授权的网络连接,其判断的依据包括 IP 分组的五元组、应用层内容等信息。而 APT 攻击者往往使用常见的应用层协议端口建立从企业内部到远程主机的 SSL 加密隧道,逃避防火墙的检测分析。
- IDS/IPS 设备难以检测采用端口跳变等躲避方法的恶意流量。IDS/IPS 设备根据已公布的恶意流量特征码来检测并阻断恶意流量,恶意流量特征码的定义主要依据应用层协议识别、流量传输特征等。在实际场景中,APT 攻击中往往采用周期性的端口跳变等方法,更进一步地将其数据传输流量模拟成常见的应用层流量,例如采用 TCP 80 端口的突发式

传输,采用 TCP 23 端口的间歇性慢速传输,隐藏其流量特征,最终规避 IDS/IPS 设备。

- 传统的日常安全审计难以应对 Oday 漏洞。目前现有的安全审计方法,着重于事前预防、事后漏洞修复缓解,不具备事中控制、识别能力。APT 攻击者所使用的 Oday 漏洞突破了事前预防,甚至让事后响应没有有效的解决办法。

3 APT 攻击的防御思路与方案设计

在 IATF(信息安全保障体系)中,一个系统的信息安全保障被划分为 4 个部分:保护、检测、响应和恢复(即 PDRR 框架),其防御思想包含被动防御和主动防御:被动防御包括反病毒软件、防火墙部署等基础安全手段;而主动防御是在被动防御的基础上,进一步实现攻击检测、攻击诱骗和溯源。在 APT 攻击面前,正是由于传统网络安全防御体系在保护和检测环节的不足,导致后续“响应”和“恢复”的无从下手。因此,总体上依然可以将 APT 攻击的防御过程纳入 PDRR 模型框架。本文从 APT 攻击的行为特征出发,采用主动控制思想力求实现对 APT 攻击的可检测性,并进一步构建符合 PDRR 模型框架的 APT 攻击防御方案,具体如图 4 所示。在方案中,包含基础安全防御和动态防御两大部分。

3.1 基础安全防御

一个设计并运行良好的基础安全防御体系是防范 APT 攻击的前提,可以大大增加 APT 攻击的难度。因为一

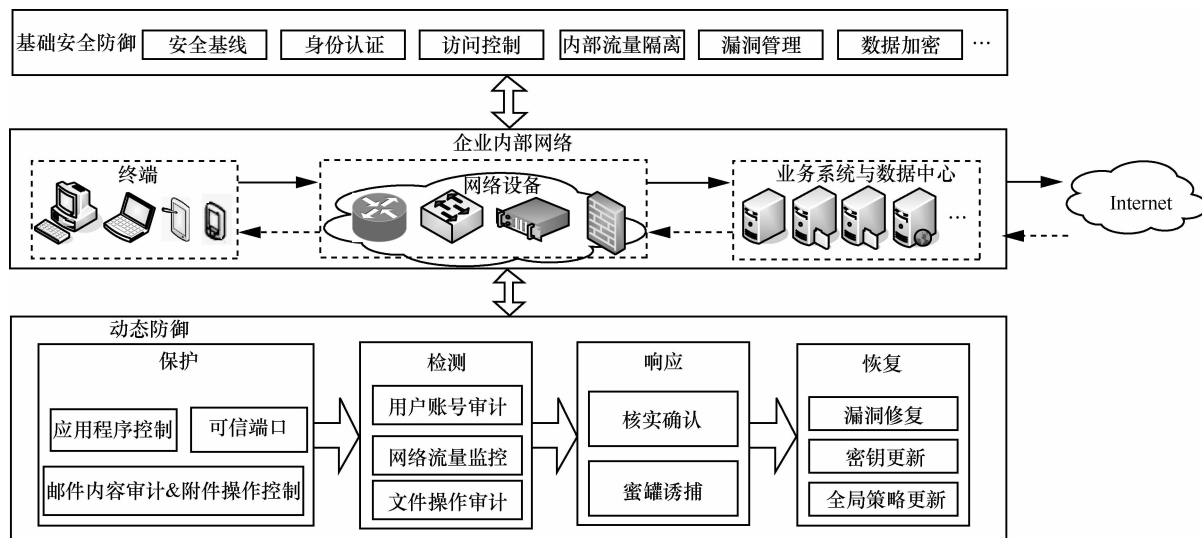


图4 APT 攻击防御方案

个企业网络若没有基本的安全防御,那么攻击者根本无需采用 APT 攻击这样代价高昂的技术手段进行信息窃取。对于 APT 攻击的防御而言,基础网络安全防御需特别关注以下安全模块的能力建设。

- 安全基线控制。通过安全基线控制可以将明文密码、SQL 注入漏洞等常见的高频漏洞清除^[2],提高 APT 攻击者的攻击门槛,延缓其在企业网络的渗透速度。
- 身份认证和访问控制。APT 攻击者以信息窃取为目的,其入侵行为往往伴随着关键文件复制等操作,而可靠有效地访问控制是文件操作审计的前提。由于 APT 攻击者常在“夜深人静”的时候利用窃取的内部员工账号进行活动,建议部署基于智能卡的身份认证(双因子身份认证)技术和强制访问控制技术。借助智能卡的物理安全性和密钥定期更新机制^[3],有效防止员工账号被恶意盗用,将大部分员工账号的使用情况与其工作时间相关联,一旦发现异常账号活动,可以快速、及时地确认处理。
- 内部流量隔离、漏洞管理和数据加密。由于 APT 攻击的长期潜伏性,建议采用等级保护的思想将重要网络流量与普通流量进行隔离保护,增加 APT 攻击者通过侦听窃取数据的难度;同时,为了阻断 APT 攻击在企业内网的渗透,应进行及时的漏洞补丁管理;最后,作为抵御 APT 攻击最后的防线,应做好对关键数据的加密,而实施的关键是良好的密钥管理体系^[3]。

3.2 APT 攻击的动态防御

APT 攻击者在企业内部网络建立攻击支点的早期阶段,没有明显的异常征兆(或者说难以被察觉);随后,其在企业内网逐步渗透,收集高价值数据资料、文件时,将带来文件操作、用户访问等行为异常,并伴随间歇性的远程加密传输;最后,当攻击者准备撤离时,需要把已窃取的高价值文件传输到远程主机。整个过程中,后两个阶段是检测 APT 攻击的最佳时机,及早检测出 APT 攻击行为并做出响应,才能尽可能避免损失,甚至可通过部署蜜罐系统最终实现攻击溯源。因此,实现对 APT 攻击的可检测能力,关键在于从日常的账号审计、网络流量监控、文件操作监控中发现异常。以下将按 PDRR 模型框架中的 4 个部分,分别进行说明。

- 保护。由于 APT 攻击的检测基于对异常数据的分析,如果不对网络流量作合理的规则划分,监控人员将难以应对日常的海量数据。因此,为了增强对 APT 攻击的防御能力,更重要的是,为降低日常监控海量数据的信息熵,给后续的审计、异常分析降低难度,同时方便统一漏洞管理,必须对终端、网络和服务设备实施基于白名单思想的策略控制,具体包括应用程序控制、可信端口控制、邮件内容审计与附件操作控制。实施办法为:只允许白名单内的应用程序安装、运行,禁止如 Skype、P2P 等存在网络端口、目的 IP 地址跳变的应用程序;只允许白名单指定端口范围内的流量发送,例如 TCP 10~5 000,UDP 10~5 000 等;采用基于内容过滤技术的邮



件网关,屏蔽垃圾邮件中的 URL 链接、附件文件,当员工要特别查看某垃圾邮件的完整内容,须向管理员申请,并备案。

- 检测。检测对象主要包括账号登录审计、网络流量监控和文件操作审计。实施办法为:由于 APT 攻击一般不会对系统的安全防御系统进行暴力破解,而使用已窃取的内部员工账号认证信息,常在“夜深人静”的非工作时间进行嗅探、渗透活动,故账号登录的时间、IP 地址等信息是重要的审计对象;由于 APT 攻击常使用端口跳变、应用层加密等手段隐藏恶意流量特征,只有通过一系列的数据聚类才能发现异常,故应在多种查询条件下对流量数据进行可视化分析,例如目的 IP 地址流量统计排序、目的端口流量统计排序等;对重要文件的操作(例如复制、移动等)及对应的时间进行审计。
- 响应。在 7×24 h 的连续监控中,一旦发现异常,须立即核实被疑似盗用的账号、已感染的主机或服务,评估已泄露的资料情况,并作隔离。在已识别控制 APT 攻击所使用的恶意程序进程的基础上,可部署蜜罐系统,诱使攻击者进入蜜罐,拖延其入侵时间,并进一步分析其行为特征、恶意流量特征,最终实现溯源。
- 恢复。在阻断 APT 攻击后,应立即请求厂商修补相关漏洞,将攻击者所植入的恶意代码提交给反病毒厂商,更新病毒库。最后应在全局做身份认证、文件加密、设备管理等方面的密钥更新、安全策略更新(例如在公司内网屏蔽社交网络等),防止 APT 攻击用同样的方法重来。

此外,APT 攻击的主动防御还需要关注人员因素,包括安全人员和普通员工:由于缺乏经验,企业的安全人员往往容易低估 APT 攻击者的能力及其手段的复杂性,而普通员工的安全意识仍需提高,须防范 APT 攻击者所发送的恶意消息。

4 典型案例

以基础安全防御为基础,结合用户终端的管理、存储系统的文件操作审计和网络流量监控等技术手段,可对 APT 攻击实现 PDRR 框架的动态防御,部署如图 5 所示。

在本示例中,通过划分安全域做好流量隔离、重要数据、文件加密存储、网络设备安全基线配置等基础安全防

御工作。其中,在内外网的流量隔离中,采取如下策略:对于无线网络接入域,禁止其访问企业内网,并只开启常用的应用协议网络端口;对于核心数据存储域,禁止外部流量对其的直接访问。在这种安全策略中,系统的安全弱点在于以固定网络接入域的主机、业务系统运行域的服务主机为跳板,可实现对企业核心数据的间接访问,这也是 APT 攻击的重要行为特征。故对 APT 攻击的可检测,关键在于实施应用程序、IP/port 白名单等控制手段后,将安全审计的对象集中于固定网络接入域主机、重要系统的员工账号,具体可采用基于异常检测的网络流量、员工账号访问审计方法。对于固定网络接入域的主机,通过从登录 IP 地址、协议端口、基于各时间窗口的流量统计等特征的统计得到该主机的内、外网正常流量模型。通过对该主机流量进行特征抽取,与其正常的流量模型比较,可得到其流量异常情况的概率值。对于被识别为“异常”概率值大的流量信息,将被推送到安全审计人员作进一步分析。类似地,对于员工账号访问审计,通过从账号登录的 IP 地址、时间、行为操作序列等特征的统计可得到该账号的正常操作行为模型,并进一步用于员工账号访问异常检测。对于异常告警,安全审计人员需及时确认原因;对于未能确认原因的异常告警信息,尤其是异常流量告警信息,需及时联系安全厂商技术支持人员进行进一步分析。

5 结束语

APT 攻击所采用的各种方法手段已超出信息安全的技术范畴,其本质是高级黑客和安全专家的信息对抗。APT 攻击在企业网络的泛滥给业界带来了深远的影响,它提升了安全服务的产业价值,对安全人员的从业素质提出了更高要求;同时,APT 攻击的检测方法,建立在对日常数据的审计挖掘基础上,对数据的可视化、快速检索提出了更高的要求,而完全异于传统网络攻击的检测方法。整体来看,APT 攻击使得信息安全的防御边界将逐步变得模糊,对它的安全防御仍有待在实践中检验和完善。

参考文献

- 1 张帅. 对 APT 攻击的检测与防御. 技术应用, 2011(9)
- 2 华汪明, 张新跃, 黄礼莲等. 电信 IT 安全保障能力评价模型与基线达标体系研究. 电信科学, 2012(4)
- 3 中国电信网络安全实验室. 云计算安全: 技术与应用. 北京: 电子工业出版社, 2012

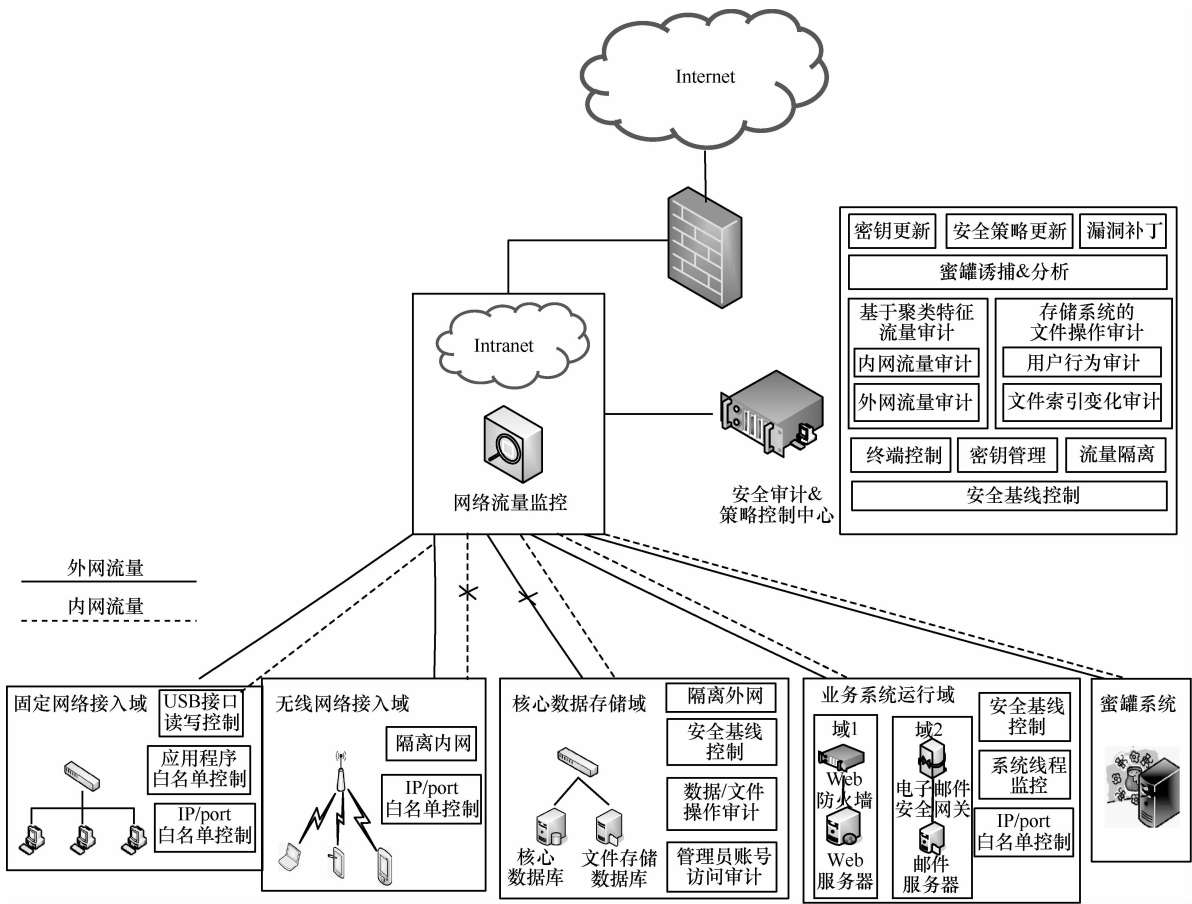
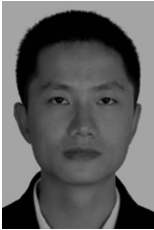


图 5 APT 攻击动态防御的部署示例

[作者简介]



刘东鑫,男,中国电信股份有限公司广东研究院工程师,主要研究方向为网络与信息安全等。

王帅,女,中国电信股份有限公司广东研究院工程师,主要研究方向为 IP 网络安全、信息安全等。

沈军,女,中国电信股份有限公司广东研究院高级工程师,主要研究方向为 IP 网络安全和网络应用安全技术等。

刘国荣,男,中国电信股份有限公司广东研究院工程师,主要研究方向为信息安全、数据库安全等。

金华敏,男,中国电信股份有限公司广东研究院高级工程师,主要研究方向为 IP 网络安全和 IT 系统安全技术等。

(收稿日期:2013-08-25)

(上接第 157 页)

规模的数据计算,解决现行流量分析系统面临的扩展性和成本问题。

参考文献

1 White T. Hadoop: the Definitive Guide. O'Reilly Media, 2011
2 Ghemawat S, Gobioff H, Leung S. The Google file system. ACM SIGOPS Operating Systems Review, 2003(5)

[作者简介]



唐宏,男,中国电信股份有限公司广东研究院高级工程师,主要研究方向为 IP 网络与云计算技术研究。

(收稿日期:2013-12-01)