金融行业安全月刊

安全月刊

07
2017 年

技术版 ▶▶ 绿盟科技金融事业部安全月刊 政策解读 / 行业研究 / 漏洞聚焦 / 产品动态

浅谈消费金融及《消费金融公司试点管理办法》解读

金融行业邮件安全解决方案

信息科技风险审计项目结合实施经验拓展审计发现

浅析信息系统生命周期安全管理体系建设思路

电子银行安全与用户体验

盘点 21 世纪以来最臭名昭著的 15 起数据安全事件

NSFOCUS

NSFOCUS绿盟科技

第25届中国国际金融展

金融行业网络安全趋势研讨

@北展报告厅 7月27日13:30-16:50

绿盟科技金融行业特装展位

@12号馆1203 7月27日-30日

不见不散

THE EXPERT BEHIND GIANTS

巨 人 背 后 的 专 家

THE EXPERT

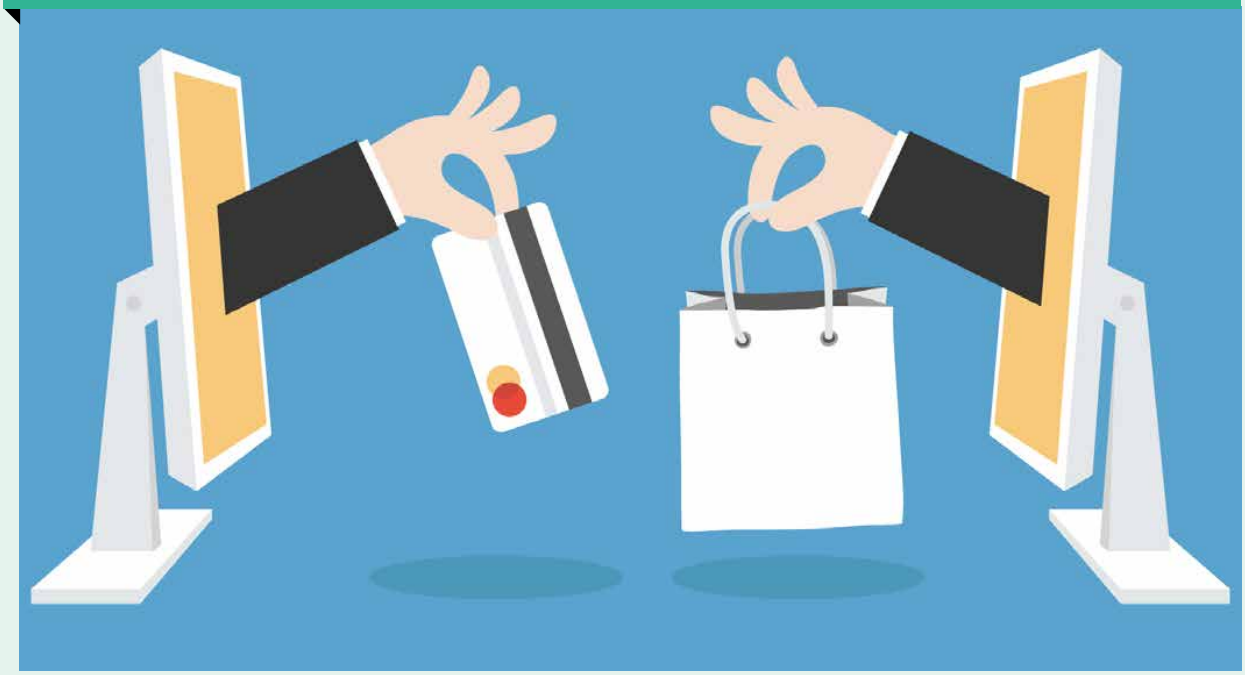
BEHIND GIANTS

巨人背后的专家

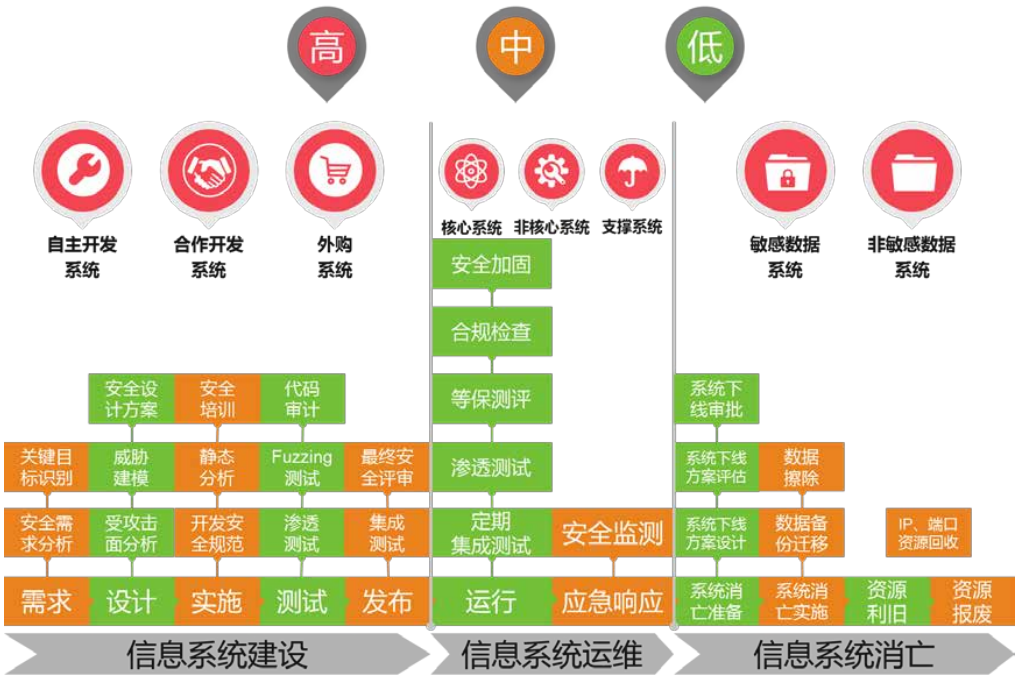
多年以来，绿盟科技致力于安全攻防的研究，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

本|期|看|点

P04 浅谈消费金融及《消费金融公司试点管理办法》解读



P26 浅析信息系统生命周期安全管理体系建设思路



安全月刊

2017年第7期

绿盟科技金融事业部

目录 CONTENTS

政策解读

行业研究

漏洞聚焦

产品动态

绿盟科技官方微信

绿盟科技金融事业部

NSFOCUS

政策解读

浅谈消费金融及《消费金融公司试点管理办法》解读

金融事业部　周扬

一、消费金融公司概述

所谓消费金融公司是指经中国银行业监督管理委员会批准，在中华人民共和国境内设立的，不吸收公众存款，以小额、分散为原则，为中国境内居民个人提供以消费为目的贷款的非银行金融机构。消费金融公司的注册门槛为3亿元人民币或等值的可兑换货币，且为一次性实缴货币资本。消费金融公司的业务主要包括个人耐用消费品贷款及一般用途个人消费贷款、信贷资产转让及同业拆借、发行金融债等。

二、关于消费金融公司的几个知道

1. 出资人资质：出资人须为境内外金融机构及银监会认可的其他出资人。其中《消费金融公司试点管理办

法》对主要出资人制定了严格的准入条件。例如具有5年以上消费金融领域的从业经验，资产总额不低于800亿元人民币，连续两个会计年度盈利，3年内不转让出资等。对于境外金融机构，还必须符合在中国境内设立代表处两年以上，且所在国家或地区金融监管当局已与银监会建立良好的监管合作机制等。

2. 业务范围：消费金融公司为居民个人提供以消费为目的的贷款，比如购买家用电器、电子产品等耐用消费品，以及用于个人及家庭旅游、婚庆、教育、装修等消费事项，但不包括房贷和车贷。

3. 贷款要求：根据《国务院办公厅关于金融支持经济结构调整和转型升级的指导意见》（国办发〔2013〕67号）规定，消费金融公司向个人发放消费贷款不应超过客户风险承受能力且借款人贷款余额最高不得超过人民币20万元。而对于此类贷款的利率，银监会表示最高不得超过央行同期贷款利率的4倍。

4. 开设原则：消费金融公司基本遵照“一省一家”的原则。一般而言，如果一个省份已经有了一家消费金融公司，就不会批准第二家。“一省一家”的原则反映了监管部门促进区域平衡发展的考虑，具有一定合理性。而在北京、上海这样的一线城市及金融中心聚集了大量的资源，存在多家共存，相关竞争的情况。

三、消费金融公司主要监管要求

1.《消费金融公司试点管理办法（修订稿）》

2.《中国银监会办公厅关于加强非银行金融机构信息科技建设和管理的指导意见》

3.《中国银监会非银行金融机构行政许可事项实施办法》

4.《国务院办公厅关于金融支持小微企业发展的实施意见》

5.《金融租赁公司、汽车金融公司和消费金融公司发行金融债券的有关事宜》

6.《关于促进互联网金融健康发展的指导意见》

四、《消费金融试点管理办法》信息科技政策解读

第六条　申请设立消费金融公司应当具备下列条件：（五）建立了有效的公司治理、内部控制和风险管理制度，具备与业务经营相适应的管理信息系统；

解读 消费金融公司的市场定位为传统银行信贷的补充，提供多种宽泛而灵活的线上和线下信贷产品，在业务飞速发展为用户带来快捷与便利的同时，也为消费金融公司的信息系统带来的更多的风险与威胁。信息系统不光承载着其核心业务，同时还生成、处理、存储着企业的核心敏感信息，例如账户信息、隐私、业务数据、金融交易记录等等。相关信息系统的安全性不足，被黑客攻击后可能导致业务中断、声誉受损，各种敏感数据还将透过地下交易流入地下经济产业链，从而造成其业务受到持续影响，给企业造成巨大的财务和信誉风险。信息系统作为消费金融公司在线开展业务的重要组成部分，是否安全、稳定的运行将直接关系到各项业务能否正常开展，因此企业应具备相关管理手段和技术措施，保护企业及用户数据的保密性、完整性及可使用性，从物理、网络、主机、应用和数据层面进行全面的安全建设及安全防护。

第二十二条　消费金融公司应当按照银监会有关规定，建立健全公司治理架构和内部控制制度，制定业务经营规则，建立全面有效的风险管理体系

解读 消费金融公司需要建立全面有效的风险管理体系，而信息科技又是消费金融公司开展业务的重要技术支撑部分，因此也有建立完善的信息科技风险管理体系的必要性。信息科技的风险管理就是对信息安全风险进行识别、分析、采取措施将风险降低到可接受水平并维持改水平的过程，企业的信息安全管理工作绝不是一劳永逸的，由于IT技术的演变，新的风险与威胁不断出现，信息安全风险管理是一个相对动态的过程，企业应做到不断改进自身的安全状态，将信息安全风险控制在一个可接受的区间内。

笔者建议消费金融公司在建立风险管理体系时可借鉴银行的体系构建模式，从信息科技治理、风险管理、外包管理、业务连续性管理、信息安全管理、项目管理建设、运行维护管理、以及IT审计监督管理等8个方面开展工作，在现有管理水平基础上，进行梳理和补充完善，建立起一套全面合规的、可落地执行的、可度量评价的信息科技风险管理体系。

第二十七条　消费金融公司如有业务外包需要，应当制定与业务外包相关的政策和管理制度，包括业务外包的决策程序、对外包方的评价和管理、控制业务信息保密性和安全性的措施和应急计划等。消费金融公司签署业务外包协议前应当向银行业监督管理机构报告业务外包的主要风险及相应的风险规避措施等。

解读 随着消费金融行业的发展以及不断加剧的业务外包需求，业务外包利用了服务提供商的专业技能和先进的管理经验，帮助企业节约了成本、提升了工作效率。与此同时，也为企业带来了更多的安全隐患，近年来外包风险事件越来越多。消费金融公司应针对当前的管理现状，从管理制度、组织架构、业务决策、评价管理、信息的保密性和安全性、应急保障计划、重点外包服务机构管理等进行全面安全评估工作。结合监管要求和行业的最佳实践，在现有管理水平基础上，进行梳理和补充完善差距分析。最终建立一套全生命周期的外包管理体系，形成有效外包风险内控机制，同时建立完善外包险管理持续改进机制，满足行业监管合规要求。

第三十一条　消费金融公司对借款人所提供的个人信息负有保密义务，不得随意对外泄露。

解读 随着2017年6月1日《网络安全法》的正式实施，将信息安全提升到了新的高度。近几年信息泄露事件呈密集高发趋势，金融行业热切关注的数据安全问题也是网络安全法的重中之重。网络安全法明确规定：网络产品、服务具有收集用户信息功能的,其提供者应当向用户明示并取得同意；网络运营者不得泄露、篡改、毁损其收集的个人信息；任何个人和组织不得窃取或者以其他非法方式获取个人信息,不得非法出售或者非法向他人提供个人信息，并规定了相应法律责任。消费金融公司应当结合自身信息系统的特点、梳理相关业务流程和数据传输路径，加强技术手段和管理措施，从个人信息的创建、存储、使用、交换、存档及销毁等方面进行全生命周期的管理工作。

NSFOCUS

行业研究

金融行业邮件安全解决方案

金融事业部　傅戈

一、前言

邮件是一个对个人和机构信息安全影响巨大的应用。个人往往容易收到各类垃圾邮件和精心伪装的网络钓鱼邮件，这些垃圾邮件和钓鱼邮件中经常包含包括病毒、木马程序、恶意链接和勒索软件在类的各式恶意代码。当前的钓鱼邮件通常采取点击诱骗、提供登录入口、内嵌附件、持续性欺骗以及高度定制化的方式来诱骗邮件接收者。而邮件接收者则出于好奇、害怕和紧急这三个最主要的人为感情因素而遭遇欺诈[1]。根据统计，在互联网中每125封邮件中就有1封邮件含有恶意软件。在2016年中，垃圾邮件及内含恶意软件的垃圾邮件数量都有上升[2]。在针对金融机构发起的攻击中，利用钓鱼邮件进行鱼叉式攻击并渗透进入内部网络是一种首选方式之一。攻击者渗透进入到银行内部网络后可以进行控制系统权限、拦截和修改数据，发送恶意指令、进行数据窃取等计算机犯罪活动。2015年卡巴斯基实验室就公布了一起通过钓鱼邮件成功入侵俄罗斯某银行而窃取ATM现金的攻击事件[3]。

此外，利用含有勒索程序的邮件进行勒索也是这几年日渐增加的一种攻击方式。根据统计，2015年中针对个人消费者的勒索攻击占到总攻击的57%，针对机构的攻击为43%。根据cisco公司研究报告显示，先进的漏洞利用平台仍然依赖于Adobe Flash软件漏洞，这些漏洞帮助勒索软件更为容易获得成功并使其成为一个突出的威胁[4]。此外，正是由于部分个人和机构向勒索者的妥协，使得勒索软件的数量剧增。Symantec公司在2014年新增发现77个家族，但在2015年则新增发现了100个家族。当前勒索软件呈现高度组织化和自助服务化的趋势。例如，一些勒索软件不仅仅通过页面提示受害者支付转账金额或比特币，它们在页面上还提供了其后台呼叫中心的服务电话号码提供提供5*8小时的电话服务指导你如何支付赎金以及如何在支付赎金后进行技术解锁操作，犯罪组织的专业性由此可见。在2015年中，地下黑产已经将勒索软件已发展成为一种勒索软件即服务的模式（Ransomware-as-a-Service, RaaS）

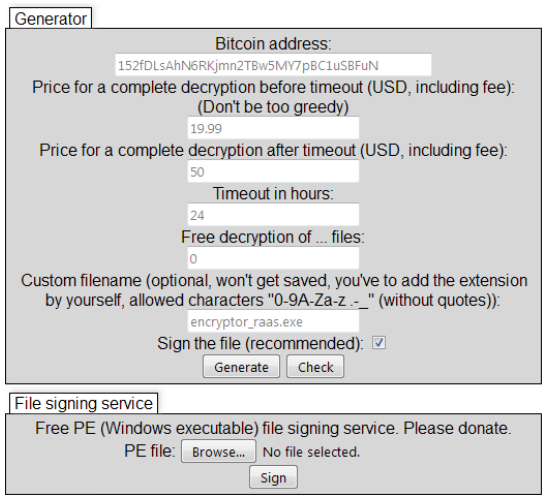


图1.1　RaaS的用户定制截图[5]

另外，勒索软件一直在进行精心的伪装并诱骗用户点击邮件附件或邮件链接。下图是cisco公司在2016年监测在垃圾邮件中最常见的社会工程欺诈主题/内容

总体而言，个人用户的警惕性不高，勒索软件的精心伪装和诱惑，对高危漏洞/零日漏洞的利用以及缺乏邮件检测过滤防护系统是勒索软件获得成功的主要因素。对于金融行业而言，勒索软件将是近期一个需要注意的方向。美国联邦金融机构检查委员会（FFIEC）和金融服务业协调委员会（FSSCC）在2015年晚些时候向美国金融服务行业就勒索软件单独发布了特别警告。而根据美国SANS机构的2016年底的一份针对金融行业机构的调查报告显示55%的机构认为勒索软件超越网络钓鱼（50%）成为首选的安全威胁之一，32%的机构反映他们损失了10万美元至50万美元不等的损失[6]。国外的一些金融机构例如英国伦敦银行甚至已经拨出专款购买比特币以防遭遇勒索软件攻击。

二、传统邮件安全防护措施的不足

前面提到，随着攻防双方的技术提升，攻击者在对金融机构发动攻击时会发现，由于金融机构较之一般企业机构更为重视信息安全，一方面暴露在互联网上的业务系统并不多，另一方面针对互联网业务系统采取了较为严密的安全防护措施。攻击者如果采取正面直接攻击互联网业务系统的方式则往往难以成功。考虑到电子邮件存在着用户之前信任、散布和发送成本低、可以集成多种攻击手段、容易进行掩盖以及邮件系统自身脆弱性等特点，因此攻击者针对金融机构的攻击更倾向于利用社会工程学通过钓鱼邮件并结合零日漏洞和恶意代码的这类攻击方式攻击渗透进入机构内部。

在传统的邮件安全中除了加强对用户的安全意识培训外，技术手段是主要的防护方式。在传统技术防护手段中“垃圾邮件整治”、“邮件服务器声誉保护”、

Version	Publication Identifier	Publication Name and URL	Message Summary	Attachment File Type	Language	Last Publication Date
96	35656	RuleID4626	Invoice, Payment	.zip	German, English	04/25/16
87	34577	RuleID10277	Purchase Order	.zip	German, English	06/02/16
82	36916	RuleID4400KVR	Purchase Order	.zip	English	02/01/16
74	38971	RuleID15448	Purchase Order, Payment, Receipt	.zip, .gz	English	08/08/16
72	41513	RuleID18688	Order, Payment, Seminar	.zip	English	09/01/16
70	40056	RuleID6396	Purchase Order, Payment, Receipt	.rar	English	06/07/16
66	34796	RuleID5118	Product Order, Payment	.zip	German, English	09/29/16
64	39317	RuleID4626 (cont)	Invoice, Payment, Shipping	.zip	English, German, Spanish	01/28/16
64	36917	RuleID4961KVR	Confirmation, Payment/ Transfer, Order, Shipping	.zip	English	07/08/16
63	37179	RuleID13288	Delivery Notice, Court Appearance, Ticket Invoice	.zip	English, Spanish	07/21/16
61	38095	RuleID858KVR	Shipping, Quote, Payment	.zip	English	08/01/16
58	39150	RuleID4961KVR	Quote Request, Product Order	.zip	English, German, Multiple Languages	01/25/16
47	41886	RuleID4961	Transfer, Shipping, Invoice	.zip	English, German, Spanish	02/22/16

Source: Cisco Security Research

图1.2　2016年垃圾邮件中最常见社会工程欺诈主题/内容[2]

“邮件病毒查杀”、“邮件内容泄密”是主要的四个防护重点，而“邮件病毒查杀”是一个主要的检测和阻断恶意代码攻击的手段。但是实践的过程里常规病毒查杀引擎存在着三个主要问题：

其一，因为加载和运行能力的限制，病毒查杀引擎并不能完全检测出已知的恶意软件。在 NTT Group 发布的《2014 Global Threat Intelligence Report》中公布了一组数字，他们采用 11 家不同的 商业和免费防病毒引擎，测试了蜜罐系统获得的恶意软件，发现高达 54% 的样本未能被检测出来。

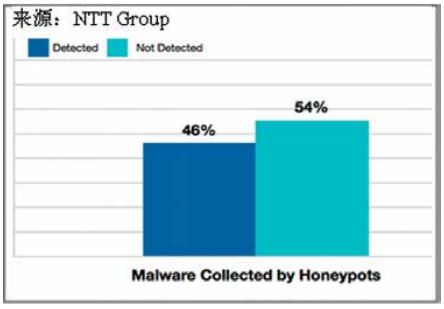


图2.1 NTT Group 检测报告[7]

其二，零日漏洞代码的利用以及其后采取多态和变形的高级攻击逃逸技术使得传统基于特征签名为基础的查杀引擎难以发现这类高级威胁恶意软件。Zeus（宙斯）木马就是一个具体的例子，Zeus 是一个金融类木马，窃取感染主机的在线交易数据，特别是网上银行帐号及交易凭据等。Zeus 木马出现于 2007 年，于2009 年被发现，但由于其不断变形的特点，虽然防病毒产品更新、添加了数以百计的检测签名，但一直未能有效控制，现今Zeus 已知变体超过 40000 余种，影响190 多个国家和地区。

其三，此外攻击者对零日漏洞的快速利用，以及用户端检测引擎更新的落后时效性也使得传统的病毒查杀引擎在应对恶意代码上检测上显得更为乏力。以CVE-2015-3113漏洞为例，国际著名的漏洞利用集成工具Magnitude在漏洞颁发仅4天后就已经集成了开源的漏洞利用代码。其利用时间早于绝大多数用户更新其安全产品规则库的时间。

因此，我们需要引进新的安全解决思路来应对利用嵌入到邮件正文链接及附件中的零日漏洞和恶意代码所发起的网络钓鱼、APT攻击和勒索攻击。

三、绿盟金融行业邮件安全解决方案

3.1 攻防技术思路

针对网络钓鱼、APT攻击、勒索软件，国内外安全界曾经提出了多种不同的检测或预防技术，安全厂商往往使用这些方法的组合来进行分析监测，这些技术包括：

- ☐ 采用深度包检测进行网络分析，如：
  - ◆ 网络通信分析
  - ◆ 多层网络流量异常、行为检测、事件相关性
  - ◆ 枚举异常IP流量（如：基于RFC等标准）
  - ◆ 恶意主机、URL基于文件信誉体系
  - ◆ 恶意软件的命令和控制通道检测
- ☐ 自动文件静态分析
  - ◆ 自动分离、解析文件对象
  - ◆ 检测嵌入的可执行代码
  - ◆ 检测逃避技术，如封装、编码及加密等
- ☐ 基于可视化、报警等进行手动分析
  - ◆ 恶意行为可视化及其分析报告
  - ◆ 可视化详细的网络流量，并关联威胁、信誉与风险级别
  - ◆ 网络流量或完整的数据包捕获上的取证分析

以上方式在使用中被发现了多个问题，包括误报率

高、大量漏报，也包括对安全管理人员的要求过高，以至于大多数组织无法使产品发挥预想的检测作用。因而这些技术方式没有被市场广泛认可。直到以FireEye公司为代表的基于虚拟执行技术的产品出现。这类产品易于部署管理、可以忽略的误报率、及时检测未知威胁，因此受到了客户的广泛认可，产品市场占有率也获得了较快的突破和发展。Gartenr组织的研究表明采用拟执行或模拟环境的检测方法是一种先进的邮件安全监测技术并且可作为传统邮件安全网关检测方式的有益补充。

该方法利用一个操作系统或浏览器实例，发起建立一个虚拟的执行容器（或者称为一个沙箱），使恶意软件和恶意链接在其中执行，就像在真实的用户环境一样。这种方式可以有效的邮件正文中的恶意链接以及邮件附件中的含有未知恶意代码的文档（如office文档、PDF、可执行文件、脚本文件等）进行检测。通过这种方式，安全产品和技术人员可以对整个攻击生命周期进行观察，从最初的漏洞利用，随后与命令控制服务器的通信，下载进一步的恶意可执行文件以及随后的网络回

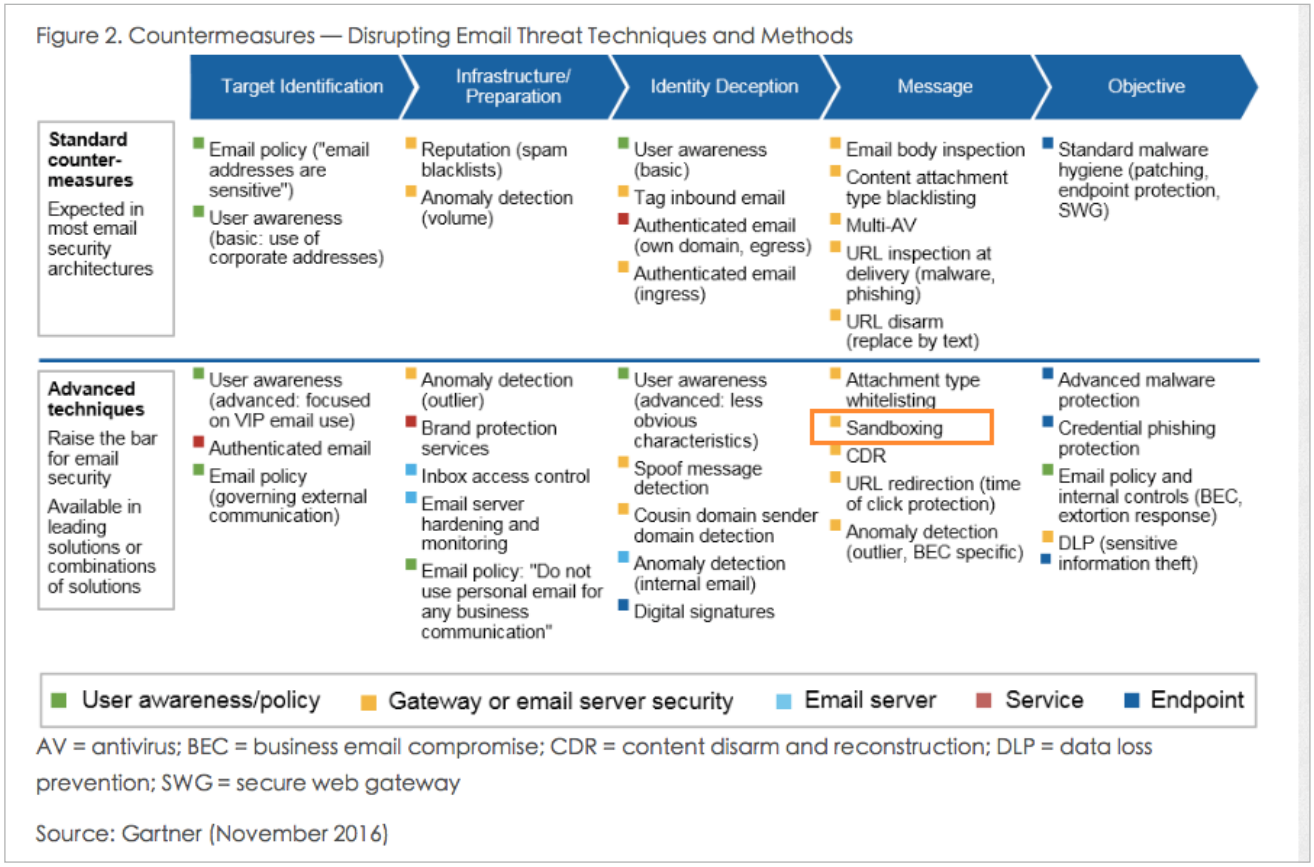


图3.1　沙箱技术是Gartner提出阻断邮件威胁的高级技术和方法

调。这种检测技术因为可以检测漏洞利用阶段的恶意软件行为，因此避免了其它只检测后期阶段活动产品的漏报（这个阶段是可以采用加密等一系列方式进行逃避）。并且因为监测是基于一个高度近似真实用户环境的恶意软件的真实活动的，因此误报率极低。良好的漏报率和误报率指标是这种基于虚拟执行环境或者沙箱的检测技术成为邮件安全中应对高级可持续威胁监测的最新和最重要的技术手段。

3.2 绿盟邮件威胁分析系统

3.2.1 产品简介

绿盟邮件威胁分析系统，英文名称为NSFOCUS Threat Analysis Center for Email（以下简称TAC-E），该产品是专门检测邮件高级威胁的网络沙箱类安全产品。该产品主要针对包含未知威胁代码的鱼叉APT攻击和勒索软件两大类高级邮件威胁。

定向的邮件APT攻击为鱼叉攻击，勒索软件是通过钓鱼邮件的方式，引诱用户点击中招。目前，勒索软件有逐渐扩散，种类越来越多的趋势。传统的防病毒产品，传统的邮件安全网关面对新的勒索软件以及勒索软件的变种很难进行检测和防护。

鱼叉APT威胁和勒索软件，这两种主要的未知恶意软件威胁，是TAC-E主要进行检测和防护的对象。TAC-E接收到可疑的邮件，会对其中的恶意URL和附件进行安全检测，在执行沙箱检测分析后，如确认没有安全风险才将邮件往后端的邮件服务器进行投递。因此，TAC-E在用户已有邮件安全网关的同时，可为用户的邮件提供第二道的安全检测和防护。

3.2.2 产品体系结构

TAC-E系统采用多核、虚拟化平台，通过并行虚拟环境检测及流处理方式达到更高的性能和更高的检测率。

系统共四个核心检测组件：信誉检测引擎、病毒检测引擎、静态检测引擎（包含漏洞检测及shellcode检测）和动态沙箱检测引擎，通过多种检测技术的并行检测，在检测已知威胁的同时，可以有效检测零日攻击和未知攻击，进而能够有效地监测高级可持续威胁。参见下图：

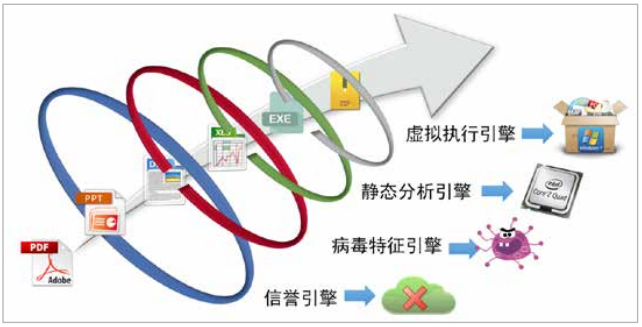


图3.2 绿盟威胁分析系统文件处理流程

3.2.3 产品主要功能

□ 邮件接收和转发

TAC-E部署在传统邮件安全网关和邮件服务器之间，接收来自外部（邮件安全网关）的邮件，经过对邮件正文和附件的过滤，再转发给邮件服务器。对邮件的接收和转发，是TAC-E的基本功能。

□ 邮件安全检测

TAC-E收到外网或者上游邮件安全网关的邮件后，对邮件进行安全检测。邮件正文中的URL和邮件附件，是安全检测的内容。

□ 邮件隔离和删除

邮件经过TAC-E检测后，如果存在恶意软件行为，可以根据策略，进行隔离或者删除操作。对于隔离的文件，可以通过邮件的方式，提醒收件人被隔离的邮件。

3.2.4 产品主要技术特点

□ 多种应用层及文件层解码

从高级可持续威胁的攻击路径上分析，绝大多数的

攻击来自与Web冲浪，钓鱼邮件以及文件共享，基于此监测系统提供以上相关的应用协议的解码还原能力，具体包括：HTTP、SMTP、POP3、IMAP、FTP。

为了更精确的检测威胁，监控系统考虑到高级可持续威胁的攻击特点，对关键文件类型进行完整的文件还原解析，系统支持了以下的文件解码：

- Office类：Word、Excel、PowerPoint…
- Adobe类：.swf、.pdf…
- 不同的压缩格式：.zip、.rar、.gz、.tar、.7z，.bz…
- 图片类：jpg、jpeg、bmp….

☐ 独特的信誉设计

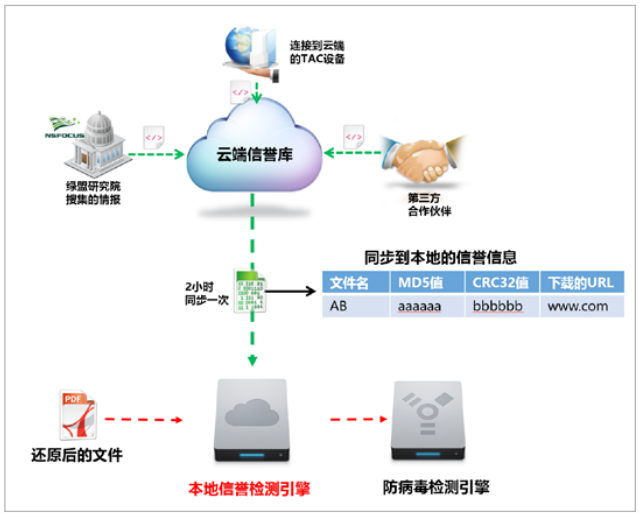


图3.3 NSFOCUS TAC-E 信誉交互过程图

TAC-E利用广阔的全球信誉，让检测更加高效、精准，当文件被还原出来后，首先进入信誉检测引擎，利用全球信誉库的信息进行一次检测，如果文件命中则提升在非动态环境下的检测优先级但不放到动态检测引擎中进行检测，如有需求可手动加载至动态检测引擎用以生成详细的报告。目前的信誉值主要有文件的MD5、CRC32值，该文件的下载URL地址、IP等信息；

☐ 集成多种已知威胁检测技术：AV、基于漏洞的静态检测

系统为更全面的检测已知、未知恶意软件，同时内置AV检测模块及基于漏洞的静态检测模块。

AV模块采用启发式文件扫描技术,可对 HTTP、SMTP、POP3、FTP 等多种协议类型的百万种病毒进行查杀,包括木马、蠕虫、宏病毒、脚本病毒等,同时可对多线程并发、深层次压缩文件等进行有效控制和查杀。

静态漏洞检测模块，不同与基于攻击特征的检测技术，它关注与攻击威胁中造成溢出等漏洞利用的特征，虽然需要基于已知的漏洞信息，但是检测精度高，并且针对利用同一漏洞的不同恶意软件，可以使用一个检测规则做到完整的覆盖，也就是说不但可以针对已知漏洞和恶意软件，对部分的未知恶意软件也有较好的检测效果。

☐ 智能ShellCode检测

恶意攻击软件中具体的攻击功能实现是一段攻击者精心构造的可执行代码，即ShellCode。一般是开启Shell、下载并执行攻击程序、添加系统账户等。由于通常攻击程序中一定会包含ShellCode，所以可以检测是否存在ShellCode作为监测恶意软件的依据。这种检测技术不依赖与特定的攻击样本或者漏洞利用方式，可以有效的检测已知、未知威胁。

需要注意的是由于传统的ShellCode检测已经被业界一些厂商使用，因此攻击者在构造ShellCode时，往往会使用一些变形技术来规避。主要手段就是对相应的功能字段进行编码，达到攻击客户端时，解码字段首先运行，对编码后的功能字段进行解码，然后跳到解码后的功能字段执行。这样的情况下，简单的匹配相关的攻击功能字段就无法发现相关威胁了。

系统在传统ShellCode检测基础上，增加了文件解码功能，通过对不同文件格式的解码，还原出攻击功能字

段，从而在新的情势下，依然可以检测出已知、未知威胁。在系统中，此方式作为沙箱检测的有益补充，使系统具备更强的检测能力，提升攻击检测率。

☐ 动态沙箱检测（虚拟执行检测）

动态沙箱检测，也称虚拟执行检测，它通过虚拟机技术建立多个不同的应用环境，观察程序在其中的行为，来判断是否存在攻击。这种方式可以检测已知和未知威胁，并且因为分析的是真实应用环境下的真实行为，因此可以做到极低的误报率，而较高的检测率。

图3.4 NSFOCUS TAC-E虚拟执行过程图

检测系统具备指令级的代码分析能力，可以跟踪分析指令特征以及行为特征。指令特征包括了堆、栈中的代码执行情况等，通过指令运行中的内存空间的异常变化，可以发现各种溢出攻击等漏洞利用行为，发现零日漏洞。系统同时跟踪以下的行为特征，包括：

- 进程的创建中止，进程注入；
- 服务、驱动
- 注册表访问、改写
- 文件访问、改写、下载
- 程序端口监听
- 网络访问行为
- ……

系统根据以上行为特征，综合分析找到属于攻击威胁的行为特征，进而发现零日木马等恶意软件。

系统发现恶意软件后，会持续观察其进一步的行为，包括网络、文件、进程、注册表等等，作为报警内容的一部分输出给安全管理员，方便追查和审计。而其中恶意软件连接C&C服务器（命令与控制服务器）的网络特征也可以进一步被用来发现、跟踪botnet网络。

☐ 完备的虚拟环境

图3.5 NSFOCUS TAC-E 虚拟环境图

目前典型的APT攻击多是通过钓鱼邮件、诱惑性网站等方式将恶意代码传递到内网的终端上，绿盟TAC-E支持http、pop3、smtp、imap、smb等典型的互联网传输协议。绿盟TAC-E内置静态检测引擎，通过模拟CPU指令集的方式来形成轻量级的虚拟环境，以应对因设备内置虚拟环境有限而导致部分文件无法运行的问题。

很多APT安全事件都是从防御较薄弱的终端用户处入手，绿盟TAC-E支持WINXP、WIN7、安卓（即将发布）等多个终端虚拟操作系统；

□ 多核虚拟化平台

系统设计在一台机器上运行多个虚拟机，同时利用并行虚拟机加快执行检测任务，以达到一个可扩展的平台来处理现实世界的高速网络流量，及时、有效的进行威胁监测。

通过专门设计的虚拟机管理程序来执行威胁分析的检测策略，管理程序支持大量并行的执行环境，即包括操作系统、升级包、应用程序组合的虚拟机。每个虚拟机利用包含的环境，识别恶意软件及其关键行为特征。通过这种设计，达到了同时多并发流量、多虚拟执行环境的并行处理，提高了性能及检测率。

图3.6 NSFOCUS TAC-E 多核平台结构图

3.2.5 产品部署

绿盟TAC-E产品部署在传统邮件网关和用户后端邮件服务器之间。与传统的邮件安全网关类似，TAC-E通过SMTP协议进行邮件的收发代理并根据安全策略进行邮件内容的安全检测和安全防护。在具体使用中用户可以自行配置邮件安全策略。TAC-E的安全策略包含两个模式，分别是告警模式和阻断模式。告警模式和阻断模式的部署场景相同，不同之处在于对恶意邮件的处理策略。在告警模式下TAC-E只进行告警，不阻断邮件；在阻断模式下TAC-E则既告警，同时又阻断。

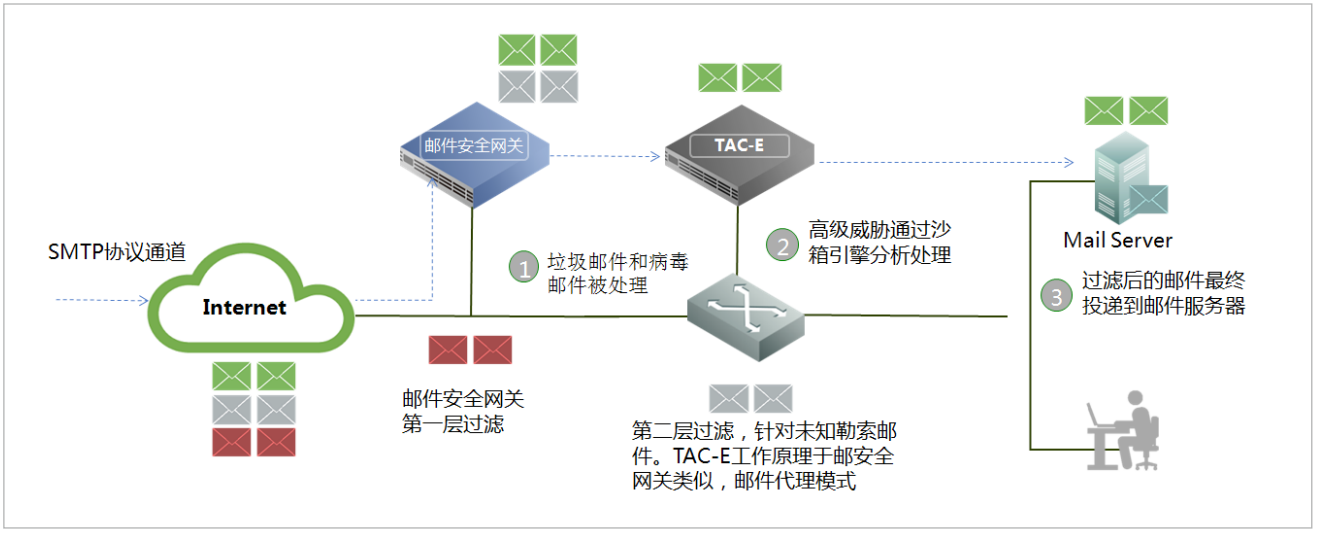


图3.7 NSFOCUS TAC-E 产品部署示意图

结束语

近年来，通过邮件进行APT攻击以及勒索软件攻击的案例呈现不断上升的趋势。从2016年的SWIFT惊天劫案以及其它曝光的国外金融机构遭遇勒索软件攻击的事件可以看到金融行业目前面临着严重的邮件安全威胁。传统的邮件安全防护措施并不足以完全应对，金融客户们亟需新一代高级可持续威胁检测防护手段。

绿盟邮件威胁分析系统/NSFOCUS Threat Analysis Center for Email（TAC-E）提供了业界领先的未知威胁检测能力，通过新一代的威胁分析检测技术，绿盟科技的产品和技术能够有效检测通过电子邮件进入网络的已知和未知的恶意软件，发现利用零日漏洞的APT攻击行为，发现恶意勒索软件代码、保护客户网络免遭这些攻击所造成的诸如内网入侵、信息窃取、数据丢失等各种风险。总体而言，绿盟邮件威胁分析系统通过降低攻击面，增加纵深安全防御的方式将有力的协助金融客户提升和加强自身的信息安全体系防护能力。

[1] “Enterprise Phishing Susceptibility and Resiliency Report 2016”

[2] “Cisco 2017 Annual Cybersecurity Report”

[3] https://securelist.com/blog/research/73638/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks

[4] “Cisco 2016 Midyear Cybersecurity Report”

[5] http://blog.imperva.com/2016/04/ransomware-as-a-service-malicious-insiders-deadly-threat.html

[6] http://www.greatlakescomputer.com/blog/ransomware-attacks-now-top-threat-to-financial-industry。

[7] 《2014 Global Threat Intelligence Report》, NTT Group

信息科技风险审计项目结合实施经验拓展审计发现

金融事业部 俞琛

摘 要： 本文以外部审计机构的视角介绍绿盟科技开展信息科技风险审计项目的实施过程，结合实施经验识别审计重点，通过使用符合性测试、实质性测试方法，强调拓展审计发现。笔者分享实施技巧，希望给予审计人员带来思路启发。

关键词： 信息系统、风险、银行、审计发现、技巧

引言

2009 年3 月，银监会发布了《商业银行信息科技风险管理指引》（以下简称《指引》），代替2006年11 月的《银行业金融机构信息系统风险管理指引》，要求各商业银行从发布之日起遵照执行。这标志着银行业信息科技风险管理工作进入了新阶段。新版监管指引的内容核心是围绕信息技术、风险管理、审计监督构成的“三道防线”IT治理架构，按照管理、执行、监督等不同职能角色的划分，建立面向主要信息科技风险类型的完整管理过程和配套管理制度体系。

在指引发布之后，银监会一方面通过非现场监管报表报送和现场检查等监管手段，促进监管要求在商业银行业务运营过程中的落实，并对落实情况进行监督检查；另一方面提倡和鼓励商业银行的审计监督部门组织实施面向信息科技风险管理合规性的内部审计和外部审计活动，切实承担起对信息科技风险管理实践的监督管理职能。

本文以外部审计机构的视角介绍绿盟科技开展信息科技风险外部审计服务项目的实施过程。结合笔者实施经验识别审计重点，通过使用符合性测试、实质性测试方法，以提高科技风险管控能力和启发审计思路，强调拓展审计发现。

一、实施过程

1.1 整体思路

从银行自身信息科技风险管理需求出发，绿盟科技依托于对行业监管规范的深入理解，以及为商业银行客户长期服务所积累的深厚行业经验，建立了商业银行信息科技风险管理外部审计的规范化实施方法和服务实施团队，向商业银行客户提供信息科技风险管理外部审计服务。

信息科技风险审计项目主要阶段包括：计划准备阶段、现场实施阶段、分析报告阶段、整改跟踪阶段。如图1所示：

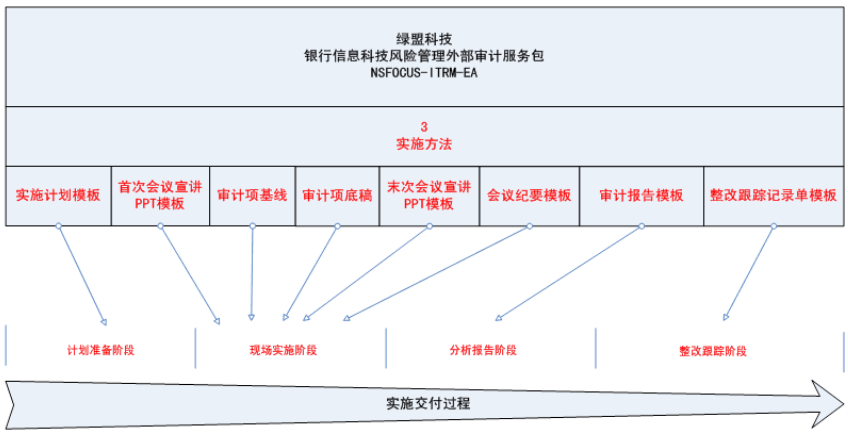


图1 信息科技风险审计项目实施过程

1.2 计划准备阶段

在计划准备阶段，需要进行的主要活动包括：

◆ 组成服务项目组，明确人员职责分工和协作方式。

◆ 开展审前调查，重点了解三道防线设立、信息科技风险管理体系的设计及运行情况，内部控制、信息安全、事件管理、外包管理、业务连续性等流程管理现状，并了解上次外部审计的审计意见。

◆ 制定项目审计实施方案、确定项目实施计划。审计方案包括审计目标、范围、审计内容，审计组成员的组成及分工，及对外部审计工作结果的利用。

◆ 明确审计重点，调整审计底稿。绿盟科技以纵向、横向对比结果作为依据，结合客户自身现状，明确审计重点，并据此调整审计底稿。

◆ 下发审计通知书，对审计项目涉及的部门下发通知书，告知审计目的及范围、审计时间、审计组长及审计组成员名单。

1.3 现场实施阶段

在现场实施阶段，需要进行的主要活动包括：

◆ 举行首次会议，向客户介绍审计实施方法和实施方案，明确客户方的接口人和资源配合要求，事先提出需科技部相关管理员在现场审计过程中陪同审计组开展工作，以对相应疑问及时作出专业解释。

◆ 下发调阅清单，收集上报材料，对非制度类文档等无法直接查阅的材料，如记录、表单、纪要、评审结论等过程文档统一编写调阅清单，由项目接口人员下发、收集。

◆ 实施现场审计，审计实施人员综合使用多种审计方法，对审计表中的现场检查各审计项进行信息调查和初步判断。

◆ 填写、确认事实确认书，对亲历现场审计的客观现场描述，在实施现场审计过程中搜集的证据，如照片、截图、文字材料，需由项目组填写事实确认书，并由被审计人员签字确认。

◆ 记录、梳理线索表，结合审计实施经验，对于利用查阅、访谈、符合性测试方法过程中发现的特殊、异常现象进行记录，可以作为拓展审计发现的专有工具。（线索表样张见3.2.2章节）

◆ 编制、汇总审计工作底稿，根据汇总的线索表、跟踪记录单、事实确认书，项目组对现状进行分析，编制审计工作底稿。

◆ 信息沟通汇总，项目组需要进行内部信息汇总与沟通，对初步审计结论进行复核，形成一致的意见。

◆ 举行末次会议，向客户传达审计项目组的一致初步意见，说明实施过程中的各项审计发现，听取客户的意见反馈，并安排后续的审计报告编写提交工作。

1.4 分析报告阶段

在分析报告阶段，主要根据现场实施形成的审计工作底稿和团队初步一致意见，编写审计报告，报告经过内部审批和批准后提交给客户。另外根据审计实施所发现的问题，为客户提供整改建议。

1.5 整改跟踪阶段

在整改跟踪阶段，项目组负责对所发现问题的客户整改措施进行跟踪，整改可包含信息科技治理、信息安全策略、内控管理制度等方面，如应急方案和业务连续性计划的修编等内容。项目组得到相关部门整改完成的反馈之后，对相应点进行确认和审核。

此阶段是一个循环优化，不断完善的过程。项目组将指导客户相关人员开展一个周期的整改跟踪过程，客户方通过循环完善信息科技治理机制、优化信息系统架构，配合安全技术加强等措施，以提高信息科技风险防范水平，做到防患于未然。

二、审计重点

银监会要求商业银行每三年全面覆盖信息科技风险审计八个方面内容，商业银行一般会邀请第三方来协助开展审计。在为银行实施外部审计项目时，项目组首先需要明确审计内容，通常会以银监会的方针政策为指引，以行业内的最佳实施准则为依据。

绿盟科技通过收集、梳理各省银监局的信息科技风险的合规要求，与银监会《指引》进行对比，以此作为行业纵向对比依据。同时，在过滤客户敏感信息后，对比分析历年的信息科技风险指标数据，统计商业银行信息科技风险管理状况，以此作为行业横向对比依据。

纵向对比发现伴随着银行业越来越活跃的各种渠道及服务方式的多样性及开放性，银行信息安全事件频发的趋势难以遏制。银行业监管机构不断出台了若干监管要求、指导意见，要求各家银行做好信息科技的技术和管理保障工作，特别针对信息科技风险管理、信息安全更是加大了监管力度。

图2 银监会要求与地方银监局要求对比（示例）

横向对比发现信息科技运行由科技部负责，对于系统、网络、基础设施的日常运行、维护工作执行效果较好，各行的机房物理环境的基础设施以及安全保障做得较为完备。信息科技风险管理方面，部分银行缺乏独立的信息科技风险管理机构与岗位，很难独立执行信息科技风险管控职能。业务连续

性方面根据各行的认知及需要逐步制订IT应急预案，部分银行开展业务影响分析指导整体策略制定。由于业务连续性内容涉及广泛，通常建议在项目实施时分步实现，首先覆盖合规要求，之后再以专项审计项目开展专门审计。

结合客户自身现状发现，部分城商系银行对于建立的信息科技委员会、风险管理委员会职能、设立首席信息官（CIO）职务的目的和职责不清晰，导致高层委员会履职情况不佳，CIO职务虚设的情况普遍存在。

绿盟科技以纵向、横向对比结果作为依据，结合客户自身现状，明确审计项目重点。笔者归纳出近年信息科技风险审计项目的审计重点包括信息科技治理、信息科技风险管理、信息安全三个方面。

2.1 信息科技治理

信息科技治理方面强调商业银行需要认真贯彻银监会《指引》要求，完善银行高级管理层设置与分工、明确信息科技规划、建立健全三道防线与相应部门的职责分工。

商业银行客户可能已实施过信息系统等保测评，由于等保的管理要求是围绕信息系统的视角来看，从管理机构、管理制度、人员安全三个方面提要求，对于岗位设置提出应设立信息安全管理职能部门，应设立系统管理员、网络管理员、安全管理员等岗位。《指引》从银行信息科技治理的视角来看，包含科技治理、风险管理、内、外审计方面的管理职能分工、岗位设置要求。因而，等保的管理要求在范围上不能覆盖《指引》要求。如果要基于等保实施成果开展信息科技治理审计，审计人员需要使用审计表中“信息科技治理”域的审计点开展补充审计。

如果项目实施过程停留在信息科技部门内部，项目将无法完成“三道防线”中的风险管理线和审计线的审计点。项目组应积极争取得到银行副行长、首席信息官、监事长的支持。

信息科技治理方面重点审计内容：

- 信息科技管理委员会、风险管理委员会职责分工、履职情况；
- 首席信息官有无确保信息安全战略、制定风险管控体制职能、及其履职情况；
- “三道防线”与相应部门的职责分工、责任边界；
- 复核内部审计执行情况，鉴证内部控制、合规性、系统安全性等方面的评价。建议审计部门职能从“纠错查弊”向“免疫功能”转变，通过完善方法论，配置信息科技风险专岗人员，配置专用工具，以提升审计能力。

2.2 信息科技风险管理

通常情况下，信息科技风险管理属于风险管理部负责。项目组应与风险管理部充分沟通、调研了解风险管理运行情况，对于风险管理模型可以提出如下问题进行审计：

- 笔者们以前是否已经识别和分析所涉及的风险?
- 在进行风险识别时，笔者们识别真正的原因了吗?
- 笔者们对风险和控制的分级和评估正确吗?
- 是否按照原计划进行控制?
- 应对计划有效吗?
- 如果应对计划无效，该做哪些改善?
- 笔者们的监测和符合过程有效吗?
- 笔者们风险管理过程总体上该如何改善?
- 哪些人需要知道这些知识?笔者们应如何传播这些知识，以确保该学习是最有效的?
- 为了确保失败的事项不再发生，而成功的事项却可以重复发生，笔者们需要做些什么?

2.3 信息安全

信息安全管理主要包括操作系统安全、应用系统安全、用户认证与访问控制、通信安全、物理环境安全等内容，安全管理是一个整体，一环出现问题，可能引起连锁反应。项目

组需要配置熟练使用技术评估工具的技术工程师开展信息安全方面审计工作。

如对于通信安全方面的审计工作需要如下三个步骤：

◆ 调阅相关管理制度文件，查看有关网络区域划分和访问控制的管理内容

◆ 调阅网络拓扑结构图，验证网络区域划分以及访问控制隔离设备的部署情况

◆ 抽样检查网络访问控制设备的配置策略适当性（技术评估，见3.1.3章节）

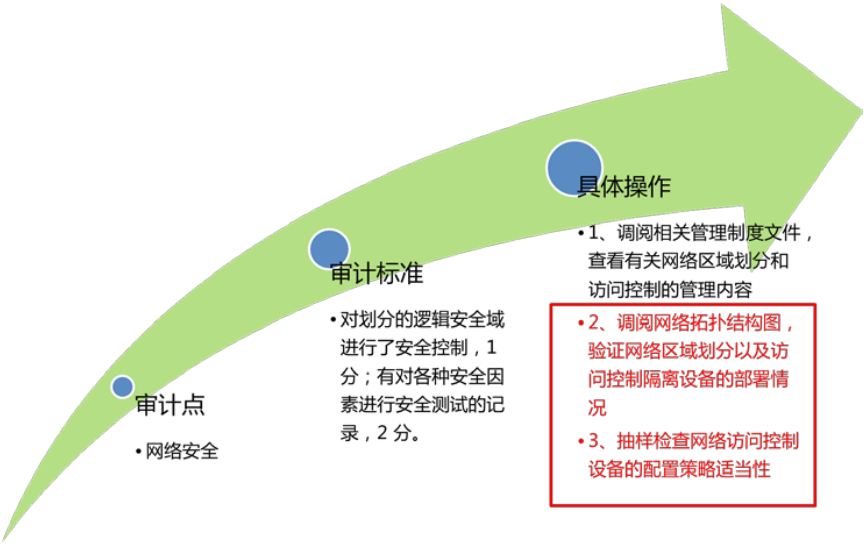


图3 网络安全审计点

三、实施技巧、实用工具

在开展审计项目过程中，需要审计人员具备项目管理的通用能力。为了提升工作效果，给予银行方面更多的成果和收获，审计人员还需要学习项目实施技巧。笔者对于实施过程中有利于预期目标实现的方法做了总结，提出实施技巧与实用工具。

3.1 实施技巧

3.1.1 项目汇报、宣贯：管理层支持，全员参与

信息科技风险计划、识别、分析、处置、跟踪等相关工作不仅是风险管理部的工作，信息技术实现、安全保障不仅是信息科技部或是信息安全组的职责。信息科技治理是由上而下，需要管理层支持。

项目组人员可以争取高级管理层、业务部门、科技部门、风险管理部门、审计部门参与到审计工作中，一些有效的方法包含：

◆ 组织高级管理层定期听取工作汇报；

◆ 提供沟通渠道使各级管理层对项目工作表态支持，并调配必要资源；

◆ 增加业务部门交流培训机会，了解行业发展趋势；

◆ 与风险管理部领导沟通，了解风险管理年度计划、风险量化与风险指标制定情况、专项风险评估计划，提出有关风险评估专岗人员的能力提升、资源投入，系统建设等议题；

◆ 与审计部门领导沟通，了解部门审计年度规划、发展路线，提出有关信息科技风险审计的人员能力提升、资源投入、工具建设等议题；

◆ 开展全员多形式安全意识、风险意识培训、宣贯。

3.1.2 信息来源：多个层面收集，拓展审计发现

信息来源由三个层面组成：

◆ 高级管理层，各委员会信息科技风险管理相关议题；

◆ 部门，三道防线各部门信息科技风险管理相关报告；

◆ 信息系统，其操作日志，及对应系统、网络设备日志；

比如调阅制度发现行内对于信息科技管理委员会、信息安全管理委员会的职责做了定义，为了识别委员会履职情况，需要使用调阅清单获取存放在审计部、科技部存档的委员会会议纪要。通过阅读纪要内容，识别出议题中不包含信息科技风险方面内容（信息科技风险方案计划评审、听取风险、事件汇报），由此项目组有了新的审计发现。

项目组人员可以争取在多个层面收集信息，结合调阅制度规范、系统、网络基线开展审计过程，通过对数据分类、分析、统计等方法拓展审计发现。

3.1.3 技术评估：发挥技术优势，拓展审计发现

技术评估内容主要包括漏洞扫描、基线检查、代码审计。其中漏扫和基检是绿盟科技传统技术评估方法。项目组需要做好技术评估前期沟通，说明漏扫的技术目的、方式和风险。比如调阅行内的AIX系统基线规范，看到有关“ICMP重定向”的基线配置要求，应设置为忽略、不发送ICMP重定向包，不转发源路由包等策略，笔者初步判断对于系统管理员如不是偏安全的出身，很大可能不重视这个策略。于是在基线检查时对比了这个策略，对比结果系统中此条策略确实没做，由此项目组有了新的审计发现。

代码审计是对系统源代码进行审计，找出编程缺陷，并提供改进建议及最佳安全编码实践。代码审计工作采用“工具扫描+人工验证”的方式，在了解业务流和各模块功能和结构的情况下，检查代码在程序编写上的安全性和脆弱性以及结构性的安全问题。项目组可配合调阅受检模块所属信息系统的设计说明书、业务流程，访谈信息系统负责人了解用户认证和访问控制、输入、输出控制环节的安全设计，一并验证其安全实现的有效性。

3.2 实用工具

3.2.1 调阅清单：合规调阅，定期统计状态

项目组在计划准备阶段和实施阶段使用调阅清单，开展非制度规范类资料调阅。为了跟踪调阅状态，表格包含了状态字段（未有、已有、现场已查阅、无记录），并在每周定期更新进展状态。调阅清单样张如图4。

需要提供调阅的资料清单（mm/dd） 记录、表单类(yy/mm/dd进展状态更新)				
编号	审计调阅资料名称	状态	拟配合部门	备注
1	同城主备数据中心（在冷凝水排水、空调加湿器排水、消防喷洒排水等管道的附近位置）装设漏水感应器情况	未有	科技部	
2	同城主备数据中心后备柴油发电机的基本容量及燃料存储量 （应保证72小时的使用需要）	未有	科技部	

图4 调阅清单样张

3.2.2 线索表：汇总梳理线索，拓展审计发现

项目组在现场实施阶段使用线索表，通过汇总梳理线索和跟踪发现，判断对应情况是否属于问题，或仅为观察项。跟踪结果（问题项、观察项、建议项）。

3.2.3 审计表：总结汇总、统一审计意见

项目组在现场实施阶段使用审计表，将审计过程发现的客观情况逐项填写在“现状描述”和“信息来源”中，对客户“管理成熟度”进行选择，将会根据“管理成熟度”的值自动生成“成熟度赋值”、“符合性分析”、“风险评级”、“差距分析雷达图”结果。

3.2.4 跟踪记录单：认真整改，持续跟踪

根据项目实施过程，整改跟踪过程属于其中必要的一个环节。只是发现问题而未及时进行整改，不仅风险不会降低，由于问题已经在一定范围内公开，反而可能提高风险，造成信息安全事件。

因而，认真完成整改工作成为必然。但待整改问题分布广泛，且属于多个部门和责任人；对于整改方案经常会做出调整，需要召集多部门人员集中讨论确定方案。通常，采用跟踪记录单并标明责任人、问题分级、整改建议、整改反馈、整改状态等列

审计过程线索表（yy/mm/dd）			
类型	线索描述	审计程序/跟踪发现	跟踪结果
治理	调阅信息科技风险管理办法、信息科技风险评估实施细则等文档发现，总行行长室信息科技管理委员会”具有负责审阅风险评估、风险处置职责，但没有履职记录；	/	问题项
运行维护	机房检查现场发现主数据中心未悬挂设备定置图，未悬挂紧急出口路线。	/	问题项
运行维护	机房检查现场发现紧急出口附近没有封条，或其他报警联动装置。	查阅视频监控发现，该紧急出口有人员进出。	问题项

图5 线索表样张

项，明确整改情况。

项目组必须严密跟踪整改进展，通过统计关键指标并适时调整整改计划，才能保证项目整体实施效果。整改状态的关键指标有：

- 有无反馈回复意见；
- 有无提供整改方案；
- 有无明确整改完成日期；

参考文献

《浅谈商业银行信息科技全面审计方法》 肖尧

《商业银行信息科技风险管理状况行业对比分析》 齐芳

结论

本文通过介绍商业银行信息科技风险外部审计项目实施过程，结合纵向、横向对比及绿盟科技实施经验，明确审计重点，分享实施技巧和实用工具。笔者希望能给正在研究和正在实施信息科技风险审计服务的人员提供思路和方法。

浅析信息系统生命周期安全管理体系建设思路

金融事业部　廖军

前言

信息技术在加速企业发展的同时，也给企业带来了各个方面的信息安全威胁；敏捷开发、快速迭代提高企业信息系统业务需求响应速度，但如何全面、有效的安全管理来提高系统的安全性也变得尤为重要。目前，部分金融机构开始尝试建立覆盖信息系统全生命周期的安全管理体系，在信息系统整个生命周期的各个阶段开展相应的安全工作，全面提高系统安全性。

本文结合目前行业现状针对企业信息系统生命周期安全管理体系的建设思路做了简单地梳理。

一、信息系统生命周期阶段划分和过程细化

根据企业信息系统开发模式进行阶段划分和过程细化是加你企业信息系统生命周期安全管理体系的先决条件。

目前主流的开发模式有两种，瀑布模型和敏捷开发

瀑布模型是指把软件生存周期的各项活动规定为按固定顺序而连接的若干阶段工作，形如瀑布流水。

敏捷开发是一种以人为核心、迭代、循序渐进的开发方法。就是把一个大项目分为多个相互联系，但也可独立运行的小项目，并分别完成，在此过程中软件一直处于可使用状态。

这里以瀑布模型为例讲述信息系统生命周期阶段划分和过程细化思路：

将信息系统生命周期分为系统建设、系统运维、系统消亡三个阶段。

各阶段子过程如下：

建设阶段：需求、设计、实施、测试、发布

运维阶段：运行、应急响应

消亡阶段：系统消亡准备、系统消亡、资源利旧、资源报废

图：信息系统生命周期

二、信息系统类型和保障级别的划分

1. 信息系统类型划分：

a) 按系统建设阶段划分：自主开发系统、合作开发系统、外购系统；

b) 按系统运维阶段划分：核心类系统、非核心类系统、支撑类系统；

c) 按系统消亡阶段划分：敏感数据系统、非敏感数据系统

2. 信息系统保障级别划分：

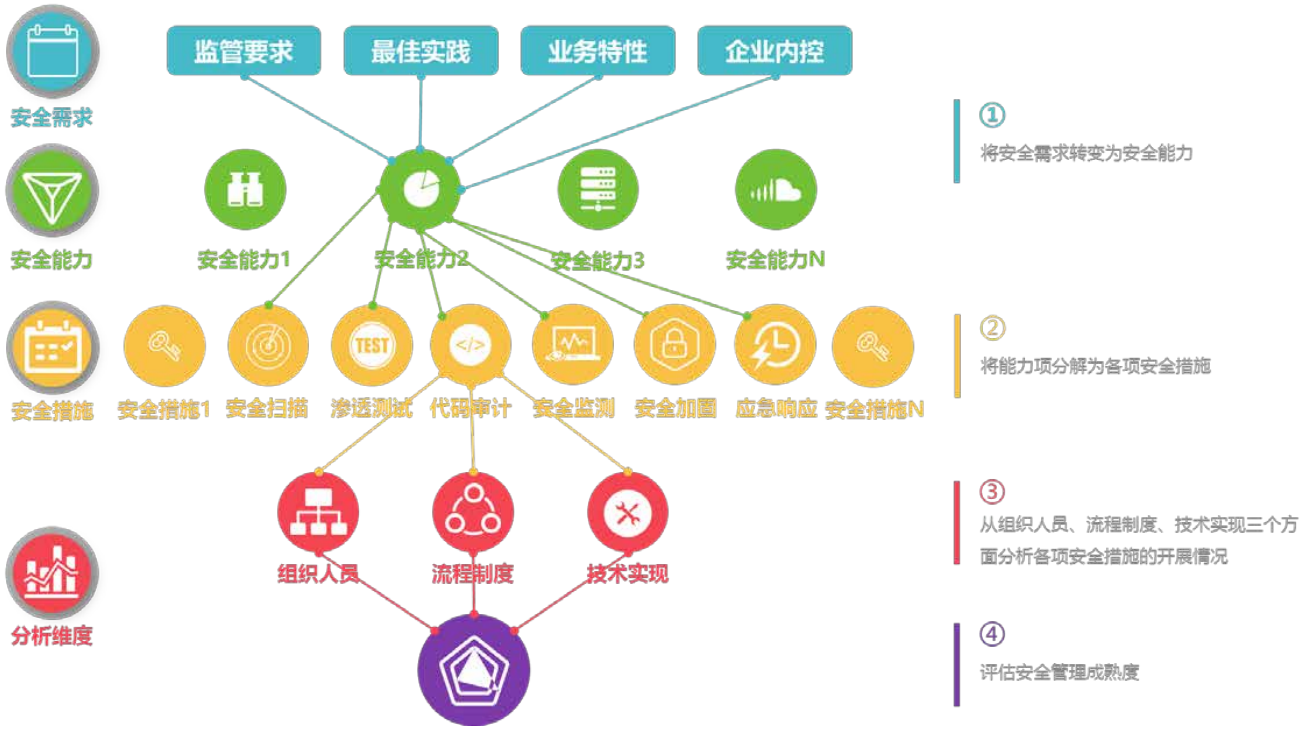
a) 高

b) 中

c) 低

三、梳理安全管理需求及安全措施

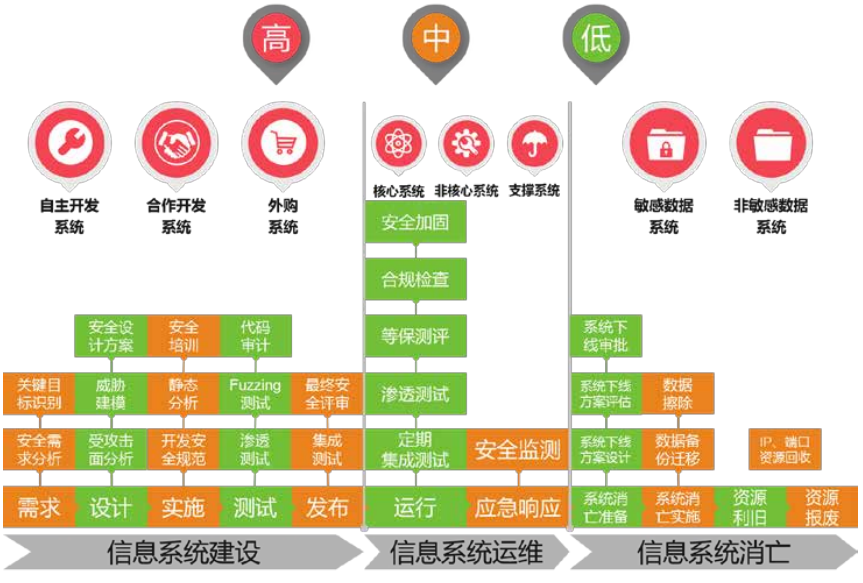
根据企业自身业务特性及安全管理需求结合行业监管要求，梳理符合企业现状的安全管理需求，将安全管理需求转变为安全能力，并将能力项分解为各项安全措施。



图：安全措施集合

四、建立信息系统生命周期安全管理体系

以信息系统生命周期为主线，信息系统类型和信息系统保障级别为对象，设计在各生命周期阶段子过程中，针对不同对象的安全管理需求，并根据按实际情况（可采取SWOT分析法）实施各项安全措施。



图：信息系统生命周期安全管理体系建立

五、运行改进

企业应按照编制的信息安全管理体系文件要求进行审核和批准并发布实施后，至此信息安全管理体系进入运行阶段。在此期间，企业应充分发挥管理体系本身的各项功能，及时找出管理体系中存在的问题，可通过对安全管理体系中各项措施的取舍（利用SWOT分析法）和信息安全能力成熟度评价，并采取纠正措施，按照更改要求对管理体系加以更改，以达到持续完善信息安全管理体系的目的。

图：信息安全能力成熟度评价

《中华人民共和国网络安全法》

第三十三条　建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

《中国银行业信息科技“十三五”发展规划监管指导意见（征求意见稿）》

第三节　增强研发运维安全管控，实现系统全生命周期安全管理

完善信息系统生命周期安全管理机制，实现信息系统从需求、开发、测试、投产上线、运行、退出的系统全流程安全管理机制。优化安全开发架构，统一部署信息安全功能，实现信息系统安全功能服务化、标准化、参数化，提升安全功能模块部署的一致性和灵活性。加强系统需求分析阶段的信息安全要求，加强新系统研发、新技术应用的安全控制，着力加强安全开发、安全测试管理。加强系统投产上线前安全评估，评价系统安全性以及对整体安全保障体系影响。

电子银行安全与用户体验

金融事业部　李桐

一、背景

在“电子银行”的范畴中，电子银行是一个更广泛的银行服务的一部分。移动商务的广泛的使用催生了各种应用软件的发展，为用户提供易于访问的信息，为用户增加各种体验经历，用的产品和良好的用户体验越来越重要。根据国际标准ISO 9241−11，UXPA（用户体验专业协会）将易用性，定义为“在指定的使用上下文中，特定用户可以使用何种程度的产品，达到有效、高效和满意的特定目标”。国际标准ISO 9241−210定义客户体验为“一个人的感知和反应，导致使用或预期使用一个产品，系统或服务”。定义进一步指出，“用户体验（UX）涉及一个人的情感，一个特定的产品、系统或服务。用户的体验包括用户人机交互的感受、情感、意义和价值。此外，它还包括一个人的认知等方面的实际应用、易用性和系统效率。”

随着应用开发水平的发展，用户越来越要求在电子银行应用中有好的易用性。因此，为了尽可能提高的用户体验，使用最佳的易用性界面和功能变得越来越重要。而电子银行使用这些界面和功能，可能面临最大的障碍是需要为用户提供高水准的用户信息安全能力。

电子银行应用程序对黑客来说，是一个包含各种漏洞的目标。因此，银行必须特别注意这些应用程序的安全性。在大多数情况下，银行能够提供安全且易用的应用程序才是客户满意度的主要标准之一。

从历史上看，多数银行都倾向于强调安全功能，提供最大的安全性。这些安全特性，在大多数情况下相当严格，并限制了用户的交易行为。这些复杂和苛刻的安全功能，可能会常见的对外部入侵的良好保护，但黑客可能通过模拟正常的用户通信，利用手机银行或互联网接入银行生产网络，从而危及内部安全。复杂的安全程序无法改变用户不安全的使用习惯，如将密码写在纸上，或利用密码记忆程序来访问他们的帐户，这可能会使银行规定的安全措施无效。对手机银行服务提供商，如何确保手机银行应用的安全性和更好的用户体验之间的平衡，越来越成为一个艰巨的任务。

二、TAM模型

近年来，越来越多的机构开始从事电子银行安全研究。为了确保网络支付的安全性，欧洲央行（ECB，2013）发布了具有14条准则的指令，2015年2月1日作为实施的最后期限。该文件指出，支付服务提供商必须对互联网支付动作和访问敏感银行数据动作进行严格的认证。“严格认证”是指由认证使用两种或两种以上的认证方式。不外乎以下三个范畴：一些用户知道的内容（例如密码），一些用户私有物品（如电话号码、智能

卡等），和用户自身特征（生物特征如指纹、视网膜、虹膜扫描等）。有了欧洲央行的指令，欧洲的银行需要引入额外的安全功能，这对电子银行来说可能会对用户体验产生负面影响。

许多国家在不同的方面进行了不同的尝试。他们用电子银行、手机银行调查用户对银行的满意度。例如，Nasri 和Cherfeddine（2012）采用信息技术接受模型（TAM）和计划行为理论（TPB）调查了用户对突尼斯网上银行的接受程度。他们强调，银行开发一种易于使用的技术非常重要，同时也强调安全和隐私。

在巴基斯坦对网络银行的研究中，作者同样认为感知的有用性和安全性已经在互联网和移动应用中大大影响银行业的发展。当用户习惯这些技术，开始经常使用网上银行，客户的满意度是主要是用户感受的易用性与有用性决定的（Mashari et al.，2014）。通过分析TAM模型的主要决定因素之间的关系（可访问性、用户信任、易用性、有用性）和网上银行用户感受，可以直接或间接影响客户的满意度。

技术接受模型（Technology Acceptance Model，TAM）是Davis运用理性行为理论研究用户对信息系统接受时所提出的一个模型。提出技术接受模型最初的目的是对计算机广泛接受的决定性因素做一个解释说明。技术接受模型提出了两个主要的决定因素：感知的有用性(perceivedusefulness)，反映一个人认为使用一个具体的系统对他工作业绩提高的程度；感知的易用性(perceivedeaseofuse)，反映一个人认为容易使用一个具体的系统的程度。

技术接受模型认为系统使用是由行为意向(behavioral intention)决定的，而行为意向由想用的态度(attitude toward using)和感知的有用性共同决定，想用的态度由感知的有用性和易用性共同决定，感知的有用性由感知的易用性和外部变量共同决定，感知的易用性是由外部变量决定的。外部变量包括系统设计特征、用户特征(包括感知形式和其他个性特征)、任务特征、开发或执行过程的本质、政策影响、组织结构等等，为技术接受模型中存在的内部信念、态度、意向和不同的个人之间的差异、环境约束、可控制的干扰因素之间建立起一种联系。

使用的态度是指个体用户在使用系统时主观上积极的或消极的感受。使用的行为意愿是个体意愿去完成特定行为的可测量程度。该模型认为目标系统的使用主要是由个体用户的使用行为意愿所决定的，使用行为意愿则是由使用态度和感知有用性决定的（BI=A+U），使用的态度是由感知有用性和感知易用性决定的（A=U+EOU），感知有用性则是由外部变量和感知易用性决定的（U=EOU+External Variables），感知易用性则是由外部变量决定的（EOU=External Variables）。外部变量是一些可测的因素，如系统培训时间、系统用户手册等以及系统本身的设计特征。

三、TAM方法的应用

在电子银行市场分析的基础上，我们基于TAM方法编制了调查问卷。问卷的第一部分包括受访客户群特征和受访者使用手机银行时的习惯。我们的目标是研究用户如何看待电子银行安全，他们所熟悉的安全功能，使用的程度，以及这些功能是否阻碍了银行交易。第二部分，通过分析样本银行的电子银行程序，我们准备了一个包含所有其手机银行安全特征，及特征组合的列表。受访者被要求提供他们正在使用的手机银行，使用过什么安全功能，以及这些安全功能是否影响或阻碍其使用手机银行。我们还比较了银行使用的电子银行安全功能差异。

有文献提出了电子银行的优质服务的六个属性：实用性、易用性、可靠性、安全性、响应能力与业务实现能力。我们的调查问卷向受访者提出了这些属性，要求他们用五分制提供他们的感受。

调查问卷中的大多数问题是封闭式，该调查是线上提供的。大量的银行客户通过不同的渠道完成问卷，从而使结果覆盖最大可能范围，我们使用了电子邮件和社交网络，如微信分发问卷，我们还请朋友和熟人做了问卷。最终收集的数据，然后使用统计方法分析。分析过程中，我们将用户提供的数据进行综合，邀请了银行安全专家，开放式收集专家的意见和建议。

四、结果分析

我们收集到了101位受访者完整的问卷调查：15（15%）的人不使用互联网或手机银行，因此排除此部分人后再进行进一步的分析。剩余的86问卷数据显示了受访者的人口统计学数据，说明了种群的多样性。每个人口数据元 ，除性别外，轻微的偏离所有人口的特点是显而易见的。年龄结构显示了最年轻和最老的受访者只占非常小的比例。在他们看来，年幼的人因年龄原因无法使用银行信用卡或网银服务，而年长的人有时会避免使用新技术，坚持传统的方式进行银行交易。受访者的教育结构显示，只有极少数的受访者为小学或职业教育水平。

受访者被要求对项目在问卷中提出了采用李克特量表（Likert scale）。开放式问卷的一部分（回复数，平均值和标准偏差）表明：受访者认为，安全功能不妨碍他们使用互联网或手机银行，受访者也有可能对他们的答复发表评论。他们的评论内容主要涉及安装耗时较长、应用的流畅程度、进入应用所需的时间和输入多个密码的问题。我们的邀请了五名银行主管参加面谈。其中3人具有多年的电子银行领域工作经验，2人曾管理过电子银行的应用的开发，1人具有金融管理硕士学位。这5人被要求按重要性列出电子银行的安全特性。

专家意见的总结表明，可用性和安全性被认为是最重要的特征，其次是可靠性、可访问性、易用性、响应能力和业务实现能力。但专家的意见相差较多。

在面谈结束时，我们提出让专家对我们的用户调查结果发表看法。调查结果并没有让他们吃惊，他们的意见是我们调查结果给出了一个用户的意见的实际情况。他们认为调查样本较少，希望能够加大调查样本量。

黑客用 U 盘启动软件让印度 ATM 机吐钱，Windows XP 再中招

随着科技的不断发展与进步，黑客与黑客方法也在“与时俱进”。不久之前，黑客通过窃取用户的信用卡信息或银行卡盗取资金。而如今，黑客借助一款开源软件让印度西孟加拉邦、古吉拉特邦、奥里萨邦和比哈尔省多地ATM机直接“吐钱”，大量资金被盗。

黑客利用一款制作USB启动盘软件——“Rufus”，无需破坏硬件，也不必窃取信用卡，就能让ATM机轻松“吐钱”，印度遭到攻击的地区因此蒙受损失。

Rufus是一个开源免费的快速制作 U 盘系统启动盘和格式化 USB 的实用小工具，它可以快速把 ISO 格式的系统镜像文件快速制作成可引导的 USB 启动安装盘，支持 Windows 或 Linux 启动。Rufus小巧玲珑，软件体积仅 7 百多 KB，然而麻雀虽小，它却五脏俱全……

Rufus除了体积小之外，它的一大特点就是「速度快」！根据官方宣称，Rufus 在制作 USB 启动盘时速度相比同类软件 Windows 7 USB Download tool、UNetbootin、Universal USB Installer 等大约能快2倍，灰常给力。

而且，Rufus完全免费开源，支持中文，官方还提供了经过微软数字签名的「绿色版」，可以不需要安装直接点开即用，非常方便。

当你需要重装系统制作启动盘时，你可以毫不犹豫

的打开 Rufus，或者你需要制作 DOS 启动盘去刷 BIOS 时都可以找它！另外 Rufus 支持 UEFI 以及 GPT 格式的安装，你完全可以在 EFI 模式安装 Windows 10、Windows 8 / 7 或者 Linux。

又是Windows XP

到目前为止，只有使用Windows XP的ATM受到影响，但并不能保证，使用其它系统的ATM就绝对安全。虽然经历过WannaCry之痛，让许多组织机构引起高度重视，但仍有大量设备在使用XP系统。Windows XP系统常被沦为攻击目标，其原因在于该系统极易遭受入侵。

此次攻击案例中，第一起事件发生在奥里萨邦，不久之后，其它地区也陆续发现了该事件。

据比哈尔警方和西孟加拉邦网络犯罪科证实，这几起攻击是网络犯罪分子所为。比哈尔警方正在咨询网络专家，希望得到相关帮助破解此案。

据报道，印度上一起ATM入侵事件发生在去年，当时采用的策略与此次类似。当时，攻击者针对的目标是贝古萨赖、吉哈纳巴德和比哈尔的巴特那。

黑客如何实施盗窃？

本次盗取ATM的这群黑客选择在夜间瞄准无人值守的ATM机。他们将被感染的随身存储器插入USB端口，以此通过恶意软件感染ATM机。此后，恶意软件会重启系统，切断与服务提供商服务器的连接。被用在ATM上之后，恶意软件还会生成代码，其可以被译为密码，当输入密码时，ATM就会吐钱，但不会立即拉响警报，黑客可以在行窃之后逃之夭夭。

安全机构指出，这类攻击之所以能够得逞，ATM厂商有一定的责任。孟买的网络律师普拉桑特马里表示，印度政府应当确保ATM制造商，印度政府增设大量ATM的同时应改善安全性。但ATM制造商否认其设备存在任何安全漏洞。

不过，这些制造商承认有几个故障案例，但这种现象并不普遍。印度储备银行目前也意识到此类情形，他们正与印度国家支付公司紧密合作，计划指导银行如何提升安全性。

文章转自：几维安全；

原文链接：http://www.kiwisec.com/news/detail/5948e92d131c530a50380a12.shtml。

专家点评

ATM恶意攻击事件层出不穷，纵观近几年类似新闻，仔细分析并未发现新型漏洞或创新攻击手法，因此我们不得不老生常谈，建议ATM厂商及银行方面从以下三个常规角度进行安全加固：

❶ 关注物理安全，尤其是外设控制：加强U盘接入控制，建议采取U盘授权机制，并对U盘执行空间进行环境安全监测，防止病毒或其他恶意程序输入；

❷ ATM操作系统安全防范：定期更新系统补丁，尤其是诸多问题的Windows低版本系统。同时按最小化服务、进程维护系统，并删除不必要的程序；

❸ 安装防病毒等终端安全防护软件：安装终端安全软件，并及时更新防护规则代码，实时监控并查杀恶意程序，保障系统安全。

盘点21世纪以来最臭名昭著的15起数据安全事件

随着互联网的普及，人们的生活也越来越数字化。例如智能家居，联网的医疗设备，网络购物，网银转账等。但技术是把双刃剑，为我们带来方便的同时，也给我们带来了潜藏的安全威胁。特别是有关人们隐私数据的泄露，也愈发严重。从个人到企业再到政府机构，数据安全俨然已经成为了我们的重中之重。下面我将为大家列举出二十一世纪以来，最臭名昭著的15起数据安全事件。注：以下列举事件并不一定是基于数量，而可能基于损害程度等进行综合评估筛选。

1. Yahoo

日期： 2013−14年

影响： 15亿用户账户

在2016年9月，曾经的互联网巨头雅虎在谈判中向Verizon推销他们时宣布，自己可能是2014年“得到国家资助的黑客攻击”事件中，史上最大数据泄露的受害者。这次泄露事件导致至少5亿用户的用户名、电邮地址、电话号码、出生日期、密码遭到泄露。雅虎表示，对其中所涉及的“绝大多数”密码，已经使用了强大的bcrypt算法进行了加密。

而在短短的几个月后，也就是十二月份，雅虎又称它们发现了新的安全漏洞，该漏洞可追溯至2013年8月，并造成至少10亿用户的姓名、电邮和密码被盗。其中涉及用户的用户名、电邮地址、电话号码、出生日期、密码，甚至还包括加密的问题及答案。

由于雅虎的违约行为，Verizon与雅虎修订了收购协议并将价格下调了3.5亿美元。Verizon最终为雅虎的核心互联网业务支付了44.8亿美元。该协议要求两家公司从违约行为中分担监管和法律责任。此次出售并未包括阿里巴巴集团报告的投资额433亿美元，雅虎日本的股份总价为93亿美元。

雅虎成立于1994年，曾被估值为1000亿美元。销售后，雅虎公司将更名为Altaba。

2. Adult Friend Finder

日期： 2016年10月

影响： 超过4.122亿账户

2016年10月中旬，成人约会和娱乐公司Friend Finder Network遭遇大规模数据泄密事件，导致4.12亿帐号信息泄露。FriendFinder包括休闲连线和成人内容网站，如Adult Friend Finder，Penthouse.com，Cams.com，iCams.com和Stripshow.com。

黑客窃取了六个数据库中，保存了近20年的数据。其中包括用户名，电子邮件地址和密码。大多数密码仅受弱SHA-1散列算法的保护。LeakedSource.com在11月14日发布了对整个数据集的分析，LeakedSource表示，该网站已经可以从数据库中提取99%的密码。

CSO Online的Steve Ragan在当时报告："根据一个名为1×0123的研究人员Adult Friend Finder的截图显示，一个本地文件包含（LFI）漏洞被触发。他表示，Adult Friend Finder生产服务器上的模块中发现的漏洞被"利用"。

AFF副总裁戴安娜·巴卢（Diana Ballou）发表声明说："我们确实发现并修复了，具有通过注入漏洞访问源代码能力的相关漏洞。

3. eBay

日期： 2014年5月

影响： 1.45亿用户受损

2014年5月，全球最大的网络交易平台之一eBay发布报告称，称数据库遭黑客攻击，至少1.45亿用户的个人资料及密码外泄。其中包括公开名称，地址，出生日期和加密密码，但被盗取的文件夹不含财务资料。该公司表示，黑客是通过三名公司员工的凭证进入到公司网络的，并保持了长达229天的内部访问权限，在此期间他们能够进入到用户数据库。

eBay要求其客户及时更改密码，同时表示财务信息（如信用卡号）是分开存储的，并没有被泄露。首席执行官John Donahue表示，违规行为导致用户活动下降，但总体影响不会太大 - 其第二季度收入增长13%，收益增长6%，符合分析师的预期。

4. Heartland Payment Systems

日期： 2008年3月

影响： SQL注入漏洞导致1.34亿张信用卡数据泄露，并导致Heartland的数据系统被安装间谍软件。

在违约发生时，Heartland正每月为175,000家商户（大多数中小型零售商）处理1亿张支付卡交易。直到2009年1月Visa和万事达，才通过Heartland中收到的可疑交易才最终发现了该问题。

其后果是，Heartland被判定为不符合支付卡行业数据安全标准（PCI DSS），并且在2009年5月之前不允许处理主要信用卡提供商的付款。该公司还为此支付了约1.45亿美元的欺诈付款赔偿金。

联邦陪审团于2009年起诉了Albert Gonzalez和两名未命名的俄罗斯共犯。Albert是古巴裔美国人，他被指控策划了信用卡和借记卡窃取的国际行动。2010年3月，他在联邦监狱被判处20年有期徒刑。

5. Target Stores

日期： 2013年12月

影响： 信用卡/借记卡信/联系信息泄露，达1.1亿人受损。

这个漏洞实际上在感恩节之前就有了，但直到几个星期后才被发现。该零售商巨头最初宣布，黑客已通过

第三方HVAC供应商进入其销售点（POS）支付卡读卡器，并收集了约4000万张信用卡和借记卡号码。

然而到2014年1月，该公司又报告称，其7000万客户的个人身份信息（PII）已经被泄露。其中包括客户全名，地址，电子邮件和电话号码。最终估计受影响的客户，达到了1.1亿。

Target的CIO也因此于2014年3月引咎辞职，其CEO也于5月辞职。该公司的违约成本估计为1.62亿美元。

6. TJX Companies, Inc.

日期： 2006年12月

影响： 9400万张信用卡被曝光。

2007年1月，零售商The TJX Companies声称它的客户交易系统遭到了黑客攻击。2003年至2006年12月期间多次遭到了入侵，黑客访问了9400万个客户账户。后来发现，有人利用窃取的信息实施了案值800万美元的礼品卡欺诈案和伪造信用卡欺诈案。2008年夏天，11个人因与该事件有关的指控而被判有罪，这也是美国司法部有史以来提起公诉的最严重的黑客破坏和身份失窃案。

TJX估计泄密带来的损失为2.56亿美元。这包括修复计算机系统以及为应对诉讼、调查、罚款及更多事项而支付的成本。这还包括因造成的损失而赔钱给维萨公司（4100万美元）和万士达卡公司（2400万美元）。

7. JP Morgan Chase

日期： 2014年7月

影响： 7600万家庭和700万企业受影响。

2014年夏天，美国最大的银行摩根大通(Jp Morgan Chase)遭到黑客攻击。这起事件共造成7600万账户信息被泄，损害了美国近一半以上的家庭，同时还对700万企业造成了影响。根据向证券交易委员会提交的文件，这些数据包括联系人信息 - 姓名，地址，电话号码和电子邮件地址以及用户的内部信息。

但是摩根大通表示，目前还没有证据显示客户的账户信息，包括账户号码、密码、用户名、生日和社会安全号码在此次攻击中被窃取。

不过，有黑客声称他们能够获取到90多家银行服务器的“root”权限，这意味着他们可以采取任何行动，包括转移资金和关闭账户。根据SANS研究所的统计显示，摩根大通每年为安全方面支出的费用，高达2.5亿美元。

2015年11月，联邦当局起诉了涉嫌参与摩根大通黑客事件的四名男子Gery Shalon，Joshua Samuel Aaron和Ziv Orenstein，他们共面临23项指控，其中包括未经授权计算机访问，身份盗用，证券和电汇诈骗以及洗钱等，估计非法获利达1亿美元。而第四位黑客的身份至今还未确定。

Shalon和Orenstein都是以色列人，他们于2016年6月承认了其罪行。Aaron则在去年十二月份，在纽约的JFK机场被捕。

8. 美国人事管理局 (OPM)

日期： 2012-14年

影响： 2200万当前和前联邦雇员的个人信息

美国人事管理局的网络被黑客入侵，约有2200万人的敏感信息（包括社会保险号码）被窃取。人事管理局在发现它的内部数据库底遭到攻击后便申请了法律调查，发现其现任、前任与潜在联邦雇员及合同工的信息均受到了威胁。简而言之，如果在2000年及之后填写了

SF-86,SF-85及SF-85P问卷的雇员，均有很高可能性遭受威胁；而在2000年之前参与背景审查的员工，也有一定可能受到波及，但概率较小。

据《纽约时报》称，来自中国的黑客从2012年开始就进入到了OPM系统，但到2014年3月20日才被发现。第二个黑客或团体在2014年5月通过第三方承包商获得了OPM许可，但直到近一年后才被发现。其中遭窃取的个人资料 - 包括详细的安全许可信息和指纹数据。

去年，联邦调查局前主任詹姆斯·科米（James Comey）谈到了所谓的SF-86表格，表示其用于对员工安全许可进行背景调查。“我的SF-86列出了自18岁以来我所居住的每一个地方，我曾到过的所有国外旅行，以及我所有家人，他们的住址等信息。”所以这不仅仅是我的身份受到影响。我有兄弟姐妹和五个孩子，他们的信息也都在那里。

内部监督和政府改革委员会去年秋天发布的一份报告总结了其所称的损害：“OPM数据泄露：政府如何危及我们的国家安全一代以上”。

9. Sony's PlayStation Network

日期： 2011年4月20日

影响： 7700万PlayStation网络帐户被黑客入侵；估计损失达1.71亿美元，同时被迫关闭网络近一个月。

这被认为是最糟糕的游戏社区数据泄露事件。 在受影响的7700万个帐户中，有1200万个未加密的信用卡号码。公司确信黑客获取了用户的全名，密码，电子邮件，家庭地址，购买历史记录，信用卡号码和PSN/Qriocity登录名和密码等信息。此外，用户在PSN平台上提交过的信用卡信息，除信用卡背面的安全码外，包括用户信用卡号码和有效期等数据也遭到了黑客的盗取。

2009年1月时，Heartland支付系统公司曾丢失1亿用户帐户信息。而此次7700万信用卡资料泄露，也使索尼事件将成为近两年最大消费者金融数据泄露案。

10. Anthem

日期： 2015年2月

影响： 导致近8000万条个人医疗数据泄露。

美国第二大医疗保险公司Anthem称遭遇黑客攻击，客户的姓名，地址，社会安全号码，出生日期和就业历史等信息遭到泄露。

加利福尼亚保险专员Dave Jones在对媒体的声明中表示，“我们的联合检查组高度证实，某国政府发起了Anthem网络攻击。另据加利福尼亚保险部1月6日率先对外发布了一份调查声明显示，Anthem公司已经为此次数据泄露付出了沉重的成本代价，其中包括250万美元聘请专家顾问、1亿1500万美元进行安全设备改进、3100万美元的受影响机构和个人的初期通报，以及为受影响用户提供的1亿1200万美元信用保护。

Anthem在2016年表示，没有证据表明会员的数据已经被出售，共享或使用。信用卡和医疗信息也均为被利用。

11. RSA Security

日期： 2011年3月

影响： 可能有4000万员工记录被盗。

2011年3月，EMC公司旗下安全部门RSA遭到安全攻击。攻击者向RSA雇员发送包含了Excel文件附件的邮件，该附件利用了一个新的Adobe Flash零日漏洞（CVE-2011-0609），触发后在受害机器上安装Poison Ivy RAT

远程控制木马。因此，攻击者获得了RSA公司内部网络的访问权，进而从网络搜集更高权限的账号，最终获得了RSA的Secur ID令牌产品的相关数据。Secure ID令牌是RSA公司的一次性密钥认证产品，有数百万企业员工使用。它提供不断变化的六位数动态密码，与常规密码一同使用，实现双密码认证。

两个月后，美国国防巨头洛克希德马丁、诺思罗普格鲁曼和L-3 Communications接连遭黑客攻击，攻击方法如出一辙，都是使用克隆的RSA SecurID令牌。有业内人士称，RSA此次遭遇攻击并不是一个小问题， 截至2009年底，约有4000万个RSA令牌被用于企业和政府网络中。除了硬件令牌，约2.5亿部智能手机在使用软件模拟令牌。现在，RSA Security 宣布替换大约4000万SecurID令牌。

12. Stuxnet

日期： 2010年的某个时间，最早始于2005年

影响： 伊朗核设施遭到破坏，并成为了针对电网，供水或公共交通系统的现实入侵和服务中断的经典案例。

2010年9月，伊朗政府宣布，大约3万个网络终端感染“震网”，病毒攻击目标直指核设施。分析人士在猜测病毒研发者具有国家背景的同时，更认为这预示着网络战已发展到以破坏硬件为目的的新阶段。伊朗政府指责美国和以色列是“震网”的幕后主使。整个攻击过程如同科幻电影：由于被病毒感染，监控录像被篡改。监控人员看到的是正常画面，而实际上离心机在失控情况下不断加速而最终损毁。位于纳坦兹的约8000台离心机中有1000台在2009年底和2010年初被换掉。俄罗斯常驻北约代表罗戈津称，病毒给伊朗布什尔核电站造成严重影响，导致放射性物质泄漏，危害不亚于切尔诺贝利核电站事故。

“震网”无须通过互联网便可传播，只要目标计算机使用微软系统，“震网”便会伪装RealTek与JMicron两大公司的数字签名，顺利绕过安全检测，自动找寻及攻击工业控制系统软件，以控制设施冷却系统或涡轮机运作，甚至让设备失控自毁，而工作人员却毫不知情。由此，“震网”成为第一个专门攻击物理世界基础设施的蠕虫病毒。可以说，“震网”也是有史以来最高端的蠕虫病毒，是首个超级网络武器。

13. VeriSign

日期： 2010全年

影响： 未披露的信息被盗

2011年秋季，全球最大SSL证书发布机构VeriSign，在呈交给美国证管会(SEC)的文件中承认2010年曾多次被黑。据称2010年时，VeriSign曾经数度遭黑客成功入侵到企业内网，并且取得小部分计算机与服务器的访问权限。

安全专家一致认为，相较于黑客的攻击行为，最令人不安的是公司的处理方式。VeriSign此前从未公布过被攻击的情况。”

VeriSign表示，没有诸如DNS服务器或证书服务器等关键系统受到威胁，但同时表示，“少部分计算机和服务器上的信息被窃取。还没有报告被盗的信息是什么，以及它对公司或客户将带来怎样的影响。

14. Home Depot

日期： 2014年9月

影响： 5600万客户的信用卡/借记卡信息被盗。

2014年9月，北美最大家居用品连锁零售集团Home Depot宣布，从今年的4、5月份开始，其POS系统就已经被恶意软件感染。

2016年3月，该公司同意支付1950万美金赔偿。包括支付1300万美金消费者损失，提供650万美金个人身份保护服务。并同意在两年内提升数据安全，增设“首席信息安全官”职位。该公司已为此泄漏花费1.52亿美金，律师费支出就高达870万美金。

该解决方案涉及约4000支付卡数据被盗的用户，以及5200万电子邮件地址被窃取的用户（两组数据有重叠）。该公司估计违约的税前费用为1.61亿美元，包括消费者结算和预期保险收益。

15. Adobe

日期： 2013年10月

影响： 3800万用户记录。

Adobe公司曾在10月初透露，黑客窃取了该公司290万客户的信息，包括他们的姓名、用户识别码和加密密码以及支付卡号，另外黑客还获得了Adobe Acrobat以及ColdFusion和ColdFusion Builder的源代码。

而后过了不久Adobe又表示，黑客访问了存储在一个独立数据库中的数量不详的Adobe ID和加密密码，Adobe表示该数据库被盗的帐号约为3800万，远远超出了月初的报道，而且该公司旗下最受欢迎的软件——Photoshop的部分源代码也被窃取。同时，黑客也窃取了客户的名称、借记卡和信用卡信息。另外据Krebs的报道称，似乎还有更多的用户信息遭泄露，可能超过1.5亿。

2015年8月，一项协议要求Adobe向用户支付110万美元违约款，已对其行和客户进行赔偿。在2016年11月，Adobe已支付给客户的款额为100万美元。

参考来源：csoonline，FB小编 secist 编译，转载自FreeBuf（FreeBuf.COM）

原文链接：http://www.freebuf.com/news/137467.html#

专家点评

纵观上述数据安全事件，随着数据资源价值的凸显，针对数据的攻击、窃取、滥用、劫持等活动持续泛滥，并呈现出产业化、高科技化和跨国化等特性，对企业乃至国家的数据生态治理水平和组织的数据安全管理能力提出全新挑战，绿盟科技建议从以下几点措施来实现数据的安全防护：

1. 定期对数据库进行安全巡检，发现数据库使用中的安全隐患，及时人工进行加固；
2. 安全管理员要了解本单位数据库中的数据资产，采取有针对性的安全防御措施，通过对数据库中的敏感字段加密存储，防“拖库”；
3. 通过技术手段实现数据库的外围防御圈，构建数据库的可信访问环境； 网络上可信：串联数据库防火墙后，黑客无法绕过数据库防火墙直接访问数据库。应用服务器可信：通过IP/MAC绑定，确保只有授权服务器、设备访问数据库。
4. 底线防守，超过阀值限制的批量查询操作拦截，绕过合法应用的访问阻断，禁止本地登录；
5. 对数据库的敏感操作，一定要全部记入审计记录，如果出现违规操作可以通过事后追责定责。

数据库已经成为数据泄漏的重灾区，在核心数据掌握企业命脉的年代，数据库的防护成为整个安防体系中不可或缺的环节。

塔塔的开发员犯低级错误，将银行的代码泄露到GitHub公共代码库上！

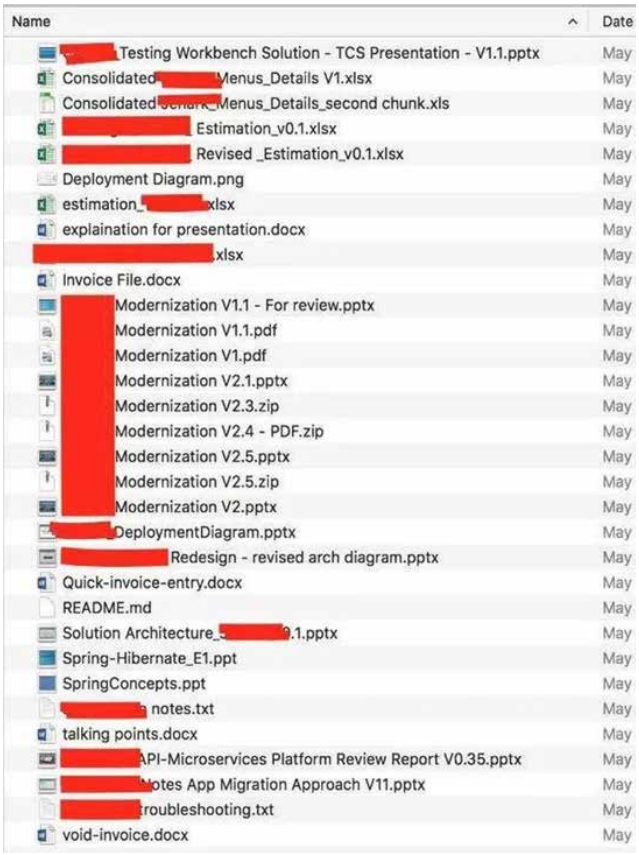
一名IT专家声称，印度外包公司塔塔（Tata）的工作人员居然将一大批金融机构的源代码和内部文件上传到了GitHub的公共代码库上。

贾森·库尔斯（Jason Coulls）是食品安全测试公司Tellspec的首席技术官，以前是一名银行软件开发员。他说，印度加尔各答的一名塔塔开发员不小心泄露了这一大堆敏感文件，后来自己无意中发现了这些文件（https://coulls.blogspot.com/2017/06/how-do-you-fix-mobile-banking-in-canada.html）。他在这批文件中看到了开发说明、原始源代码、关于网络银行代码开发计划的内部报告以及与外包合作伙伴之间的电话记录。

这些文件涉及塔塔为六家知名加拿大银行、两家著名的美国金融机构、一家跨国日本银行以及一家年收入高达数十亿美元的金融软件公司从事的编程工作。无论对于可能利用设计中任何缺陷、进而窃取数百万美元的犯罪分子而言，还是对于正在开发类似产品功能的竞争对手而言，这些数据都异常宝贵。

库尔斯上周告诉英国IT网站The Register：“好消息是，这些数据没有一个是银行客户的数据，主要是辅助数据。”

“不过里面还是有好多有用的资料——不仅对于黑客而言如此，对于这家公司的竞争对手而言也是如此。有人在常识方面犯了个天大的错误。”



这么多信息足以导致严重的破坏行为……该屏幕截图显示了部分泄露的数据；出于安全考虑，作了一番编辑。

接到泄密警告后，你以为那些受影响的公司会迅速作出反应，然而，实际情况并非如此。现住在加拿大多

伦多的英国人库尔斯表示，他将情况告知那些加拿大银行后，居然吃了闭门羹，或者无人理睬。

我们获悉，相比之下，美国金融机构非常迅速地接受了忠告，并立即作出了回应。那些泄露的文件很快从GitHub上删除了。塔塔没有回应The Register要求其评论的请求。目前，出于安全考虑，受影响客户的名称并未透露。

加拿大银行怎么啦?

库尔斯告诉The Register，他遇到加拿大银行毫不妥协的情况不足为奇——多年来，他一直对加拿大银行松懈的安全措施颇有微词，也没有看到多大的改进。

他解释道：“加拿大与美国存在巨大的文化差异。加拿大人不想为安全信息掏钱，我又不是无偿工作。而相比之下，美国公司会派人员搭飞机前来多伦多，当天晚上请我喝酒，与我讨论这个问题。“

库尔斯写过一本内容关于加拿大银行软件的电子书（https://www.amazon.com/Not-monkeys-circus-Jason-Coulls-ebook/dp/B06XXQYK6R），题为《不是我的猴子，不是我的马戏团！》。他说，他的研究表明，25家加拿大Schedule I银行中有9家很容易受到网络钓鱼攻击。

他说，有一家银行的应用程序“泄露了大量的数据——每次事务操作会将40MB的数据发送给浏览器。”他表示，也很少有移动银行应用程序努力为通信内容确保安全。

加拿大商业金融公司银行：丰业银行（Scotiabank）就是库尔斯重点炮轰的一个对象。他告诉我们，这家银行的应用程序并不总是使用HTTPS用于网络连接，而是使用不大安全的HTTP。

他说：“现在至少有一百万人在使用不安全的移动银行应用程序，早晚会出大娄子。这方面的情形并不乐观，有人迟早会追悔莫及。”

文章转自：sohu搜狐；

原文链接：http://www.sohu.com/a/148367882_465914。

专家点评

不管有意无意，泄露的数据就在那里；不管有用没用，竞争对手与黑客已经盯上你！银行外包风险管理不能仅停留在制度上，还要与实际情况结合，规范外包方开发环境和资料获取的权限，在数据泄露的源头上预防。银行研发数据加密、脱敏、外发与文档权限的管理，是重要的防范手段。加强重要数据外发的记录、审计和事后追责，才能最终堵住泄露的数据，减少损失。当然，这一切都源于你是否对“数据安全”这事走心。

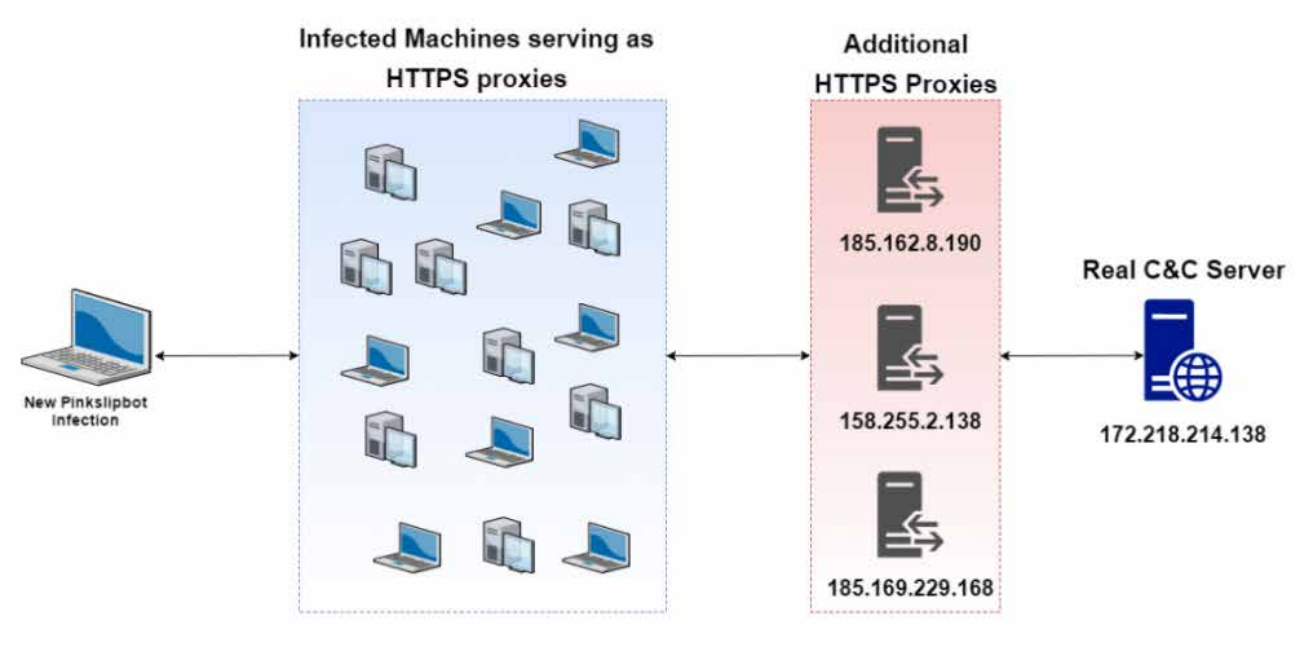
新型银行恶意软件 Pinkslipbot 利用受感染设备作为“HTTPS 控制服务器”通信

据外媒 6 月 19 日报道，McAfee Labs 安全研究人员发现一款新型银行恶意软件 Pinkslipbot（又名：QakBot / QBot）可使用复杂多级代理通过 “HTTPS 控制服务器”通信。

Pinkslipbot 最初于 2009 年被赛门铁克检测曝光，是首款利用受感染机器作为 HTTPS 控制服务器的恶意软件。此外，Pinkslipbot 还是一款具有后门功能的爬虫，可在采集登录凭证的僵尸网络中聚集受感染设备。近期，Pinkslipbot 变种新增了高级规避检测功能。

安全专家注意到，Pinkslipbot 使用通用即插即用（UPnP）功能为目标设备提供路径，以感染恶意软件 IP 地址列表中提供的 HTTPS 服务器。这些设备充当 HTTP 代理并将路径传输至另一层 HTTPS 代理，能够允许对真实的 C&C 服务器 IP 地址进行伪装。

据悉，该恶意软件只能使用美国 IP 地址利用 Comcast Internet 测速仪检测目标设备是否连接。如果目标通过速度测试，恶意软件将点击 UPnP 端口检查可用服务。目前，研究人员尚未分析清楚攻击者如何判定



“受感染设备有资格成为控制服务器代理”的确切程序。

研究人员认为，评价结果或将取决于受感染机器是否满足三个条件，即 IP 地址位于北美、高速上网以及使用 UPnP 打开 Internet 网关设备端口的能力。一旦检测到可用端口，恶意软件将感染防火墙后的目标设备并通过建立永久端口映射路由流量，旨在起到 C&C 代理的作用。

目前，受感染机器从新 Pinkslipbot 感染源接收到控制服务器请求后，立即通过使用 libcurl URL 传输库的附加代理将所有流量路由传输至真实控制服务器中。为防止设备感染该恶意软件，用户应保留本地端口传输规则，并仅在必要时打开 UPnP。

原作者：Pierluigi Paganini， 译者：青楚，译审：游弋文章

转自 HackerNews.cc ，原文链接：http://hackernews.cc/archives/11504。

专家点评

一般情况下，主机或设备上的通用即插即用（UPnP）功能是默认可信的，不会提供安全保护措施。但事实上UPnP功能非常容易被恶意程序利用，Pinkslipbot就是个非常典型的例子。因此，目前我们建议的可行有效之法就禁用UPnP功能，来避免受到黑客的非法入侵了。但如果要彻底解决类似问题需要针对UPnP功能建立完善的安全机制，防止被恶意程序利用。毕竟UPnP功能可以比较简单的实现各种设备的常见对等网络连接，有一定实用价值。

银行恶意软件 QakBot 导致大量 Active Directory 域被锁定

近日，IBM公司的恶意软件研究人员注意到，成百上千个Active Directory用户被锁定在其公司的域名之外，而此次事件正是由Qbot银行恶意软件所造成的。

关于Active Directory

活动目录（Active Directory）是面向 Windows Standard Server、Windows Enterprise Server 以及 Windows Datacenter Server 的目录服务。它存储了有关网络对象的信息，并且让管理员和用户能够轻松地查找和使用这些信息。Microsoft Active Directory 服务是Windows 平台的核心组件，它为用户管理网络环境各个组成要素的标识和关系提供了一种有力的手段。

Qbot魅影重现

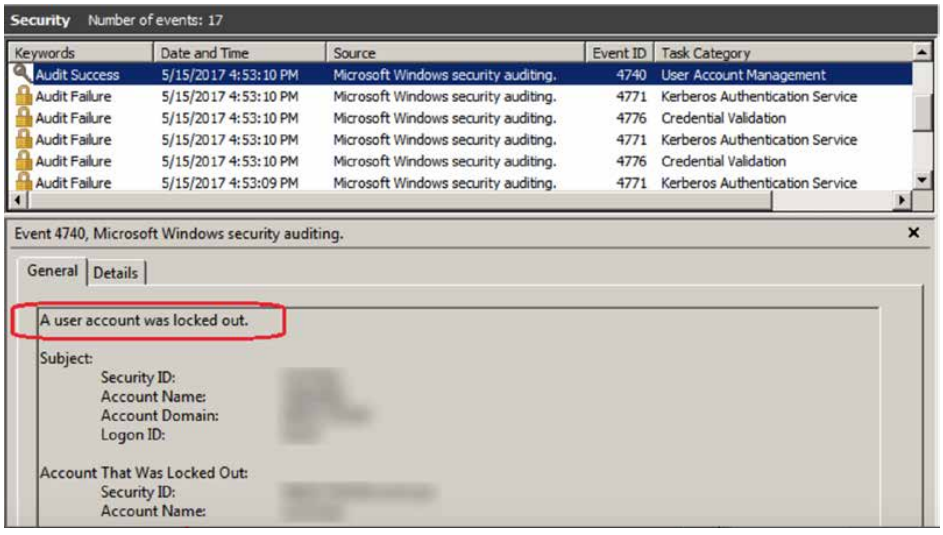
据悉Qbot（又称QakBot）银行恶意软件首次出现于2009年，并随着时间流逝不断地得以改善演变。Qbot银行恶意软件旨在针对企业银行账户，窃取用户资金，其主要通过共享驱动器和可移动设备来实现网络蠕虫功能。

除了窃取用户账号资金外，Qbot银行恶意软件还可以窃取用户个人数据，如数字证书、按键信息、缓存凭证、HTTP（S）会话认证数据、Cookie、身份验证令牌以及 FTP和POP3 登录凭证等。

近期，该恶意软件主要针对美国商业银行服务开展攻击活动，包括美国国家财政部（treasury）、企业银行以及商业银行等。

根据IBM发布的博客文章所示，

这是IBM X-Force研究小组第一次发现恶意软件可以导致AD被锁定在受影响的企业网络中的案例。



IBM研究人员表示，

QakBot是模块化的多线程恶意软件，其各种组件可以实施网上银行凭证盗窃、后门功能、SOCKS代理、深度的反取证能力以及破坏反病毒（AV）工具的能力等。除了完善的逃避技巧外，如果给予其管理员权限，QakBot当前的变体还可以禁用端点上运行的安全软件。”

QakBot银行恶意软件实施了特殊的检测机制，利用快速突变（rapid mutation）来规避反病毒工具检测。

IBM进一步解释称，

在感染新的端点后，该恶意软件会使用快速突变来规避AV系统检测。通过对恶意软件文件进行细微的修改，以及在其他情况下，重新编译整个代码，以便使其看起来无法识别。

此外，QakBot银行恶意软件还利用dropper进行传播该恶意软件，研究人员发现，它使用延迟执行（10至15分钟）来逃避检测。据悉，dropper执行了一个explorer.exe实例，并将QakBot动态链接库（DLL）注入到该进程中，以破坏其原始文件传播恶意软件。

dropper使用ping.exe实用程序调用一个ping命令，它将在一个循环中重复六次：

C:WindowsSystem32cmd.exe”/cping.exe −n 6 127.0.0.1 & type
“C:WindowsSystem32autoconv.exe” à
“C:UsersUserNameDesktop7a172.exe

一旦ping完成，原始QakBot dropper的内容将被合法的Windows autoconv.exe命令覆盖。QakBot使用注册表运行键（Registry runkey）和计划任务（scheduled tasks）在目标计算机上获益。为了在目标网络中进行传播，QakBot银行恶意软件还使用 C&C服务器的特定命令来实现自动和按需的横向移动。

IBM研究人员继续分析道，

为了访问和感染目标网络中的其他计算机，QakBot可能会收集受感染计算机上的用户名，并使用它们来尝试登录域名中的其他计算机设备。如果恶意软件无法从域名控制器和目标计算机中枚举用户名，恶意软件将会使用硬编码的用户名列表。

此外，该恶意软件还可以利用“浏览器中间人”（Man−in−the−Browser，简称MitB）攻击，将恶意代码注入到在线银行会话中，以便通过其控制的域名中获取脚本。

本文翻译自：http://securityaffairs.co/wordpress/59714/malware/qakbot−banking−malware−ad−attacks.html；

转载来源于嘶吼：http://www.4hou.com/info/news/5209.html。

专家点评

目前针对银行等大型金融机构的恶意软件呈现高发态势，QakBot是一款经过多年完善演变的恶意软件。其特征是传播能力和自我隐藏能力强，且能利用快速突变逃避AV检测。此类恶意软件的防护应做好以下几点：从源头上阻断，关注邮件附件、未知链接以及物理移动存储介质；严控网络传输路径，建立白环境；关键数据的加密防护，做到泄而不露；结合威胁情报阻止非法外联。

银行卡盗刷黑产链：一天发3万木马短信 月入可达十几万

在银行卡盗刷的黑色产业链中，1990元只能算一笔“小买卖”：从伪基站群发木马短信诱导用户点击链接，到钓鱼网站和拦截码“钓出”用户信息，再到“洗料人”通过多种通道将钱“洗白”分赃，银行卡盗刷产业链已经分出了泾渭分明的三块“业务”，每个业务上的黑产从业者各司其职，在几乎为零的成本背后，是“月入十几万”的利润诱惑。

这是两高首次就打击侵犯公民个人信息犯罪出台司法解释。根据此次司法解释，非法获取、出售公民个人信息，情节严重者可获刑。5月9日，最高人民法院通报了《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》。

“近年来，侵犯公民个人信息犯罪仍处于高发态势，而且与电信网络诈骗、敲诈勒索、绑架等犯罪呈合流态势，社会危害更加严重。”最高法相关人士称。

我们几乎每个人，都曾被推销电话、诈骗短信骚扰过。去年发生的“徐玉玉案”，即是个人信息遭侵犯导致的“恶果”。

在此节点，新京报推出关于“个人信息泄露”的系列调查报道。我们将通过对航空、征信、银行卡等领域的调查，以期找到个人信息泄露的源头。

直到5月23日收到电子账单，刘晓静（化名）才发现自己的信用卡被盗刷了。“我在今年2月底申请的卡，5月初激活的，但5月4日就在不知情的情况下被刷走了一笔1990元的账单，此后又有好几笔被转走。”她告诉新京报记者。

刘晓静不知道的是，她的信用卡信息已经泄露了，泄露渠道极有可能是在登录银行网站填写信息时，遭到了虚假网站“钓鱼”。

新京报记者调查了解到，在银行卡盗刷的黑色产业

链中，1990元只能算一笔“小买卖”:从伪基站群发木马短信诱导用户点击链接，到钓鱼网站和拦截码“钓出”用户信息，再到“洗料人”通过多种通道将钱“洗白”分赃，银行卡盗刷产业链已经分出了泾渭分明的三块“业务”，每个业务上的黑产从业者各司其职，在几乎为零的成本背后，是“月入十几万”的利润诱惑。

伪基站发诈骗短信 一小时收费500元，包天4500

6月6日，打开手提电脑，看着屏幕里的数字在3秒内从0跳到34，旁边的一部安卓手机发出了“滴滴”的短信提示音，小张知道，伪基站已经开始正常运作了。

屏幕上的数字显示的是他手中设备向外发送出的短信数量，每一个数字的跳动都意味着附近有人接收到了他发出的信息。

“并不是每个人都会看这条短信，”小张说，“但总有人会看，也有人会点击里面的链接。”

当天，小张发出的信息是“工商银行积分兑换活动开始，尊敬的用户，您可用积分4678分，兑换467.8元，点击官网链接兑换，”短信中还附有一个开头为95588的网站链接。

与正常的银行提示不同的是，里面的链接指向的并非工行官网，而是一个钓鱼网站，只要进入这个网站并下载所谓的安全控件，点击人的银行卡信息就会泄露出去。

也许，1000个人中只有100个人会去看这条信息，100个人里只有10个人会点击链接，但对小张来说，只要有10个人点击，就够了。

因为小张一天平均可以发出的信息数量，是三万条。

一位互联网黑产从业者表示，伪基站是银行卡盗刷产业链的上游，“伪基站，顾名思义，是可以伪装成运营商基站的设备。它一般由主机和笔记本电脑、短信群发器、短信发信机等相关设备组成，可以搜取以其为中心、一定半径范围内的手机卡信息，并任意冒用他人手机号码强行向用户手机发送编辑好的信息，伪装成10086、四大行客服都可以。”

小张在接到发“黑料”的业务时都显得很谨慎。

“你要发的内容是黑的还是白的？黑的要多收费。”6月6日，小张这样询问前来咨询“业务”的记者。

上述互联网黑产从业者透露，所谓“黑”就是发送含有诈骗内容的短信，而“白”则是商户促销等信息。在收到“发送黑料”的回复后，小张表示，一小时收费500元。“一般的老板都包天，从上午九点半发到晚上八点半，一天收费4500。”若按此计算，小张一个月可以获得十三万多的收入。

6月4日，新京报记者曾联系到几家卖伪基站的“科技公司”，公司老板称，基站有车载式，也有背包式，一台基站视功率、大小不同价格也不同，在6000元至1万元间浮动，“价格不算贵，而且只要你找到了好老板，一天就可以回本。”

小张的设备属于“车载式”，他说，只要把设备放在车里，然后去人流密集的地方把设备打开兜圈子就行。“有时会遇到警车，只要机灵点，及时把设备关掉就可以了。”

但现在伪基站越来越容易被检测出来。2016年4月，国内某安全公司在首都网络安全日展会上曾展示了伪基站追踪系统，北京地图上显示出了许多黄点和红点，从图中可以看到东城区和朝阳区的“点”最多，据介绍，这些都是伪基站活动的痕迹。

一家贩卖伪基站设备的“科技公司”在广告上赫然

显示，目前已经推出了可以过杀毒软件、智能手机甚至包含“安全自毁系统”的新型伪基站。

“我们针对伪基站其实一直在升级防范类的软件，但是有时我们研制了一款软件出来，就发现伪基站已经更新了好几代了。”一家安全防护科技公司的研究人员说。

某黑产群“洗料人”在招揽生意。

木马拦截用户短信，钓鱼网站1000元“租”一个月

当小张通过伪基站将短信轰炸式发送到手机用户手中时，不知情点击短信链接的用户就会掉入小张的“雇主”们精心设计的骗局中。

资深黑客“惊云”（化名）就是小张的雇主之一。6月2日，新京报记者联系到了“惊云”。在黑客圈混了四五年，“惊云”精通源代码编写和网站搭建，但他最主要的业务却是开发钓鱼网站。

在“惊云”演示的一款“工商银行钓鱼搭配拦截码演示”视频中，他制作了一个域名为“95588”的网站，网站界面几乎和工商银行官网一模一样。

谈到做网站的价码，“惊云”说：“搭建钓鱼网站1000元一个月，手机短信拦截码500一个月，手机感染软件周租带链接整套1200一周。”

“域名是可以自己编写的，把95588、95555这种银行客服电话写进去是很容易的，只不过后缀不能是.com，只能用别的。”他说，“我们只要在这个网站里加上‘积分兑换’之类的内容，诱导‘鱼’来填写账户密码就好了。”

“惊云”所说的“鱼”，指的就是受骗填写自己银行卡信息的手机用户。

在“惊云”的演示中，当他在钓鱼网站点击“积分兑换”选项时，会出现要求填写用户身份证、手机号、银行卡账户和密码的选项，填写完后，这些信息都会发到“惊云”的另一个软件后台。“这样，‘鱼’就上钩了。”

用户填写完这些信息后，钓鱼网站还会以“需要安装安全控件”为名诱导用户安装手机木马。“不管‘鱼’填写安装还是不安装，手机木马都会自动开始安装，这样我们就可以把短信拦截木马植入到用户手机中。”“惊云”说。

在银行卡盗刷黑市里，用户的身份证、手机号、银行卡账户和密码被称为“四大件”，被植入了手机短信拦截木马的用户，黑客可以轻易拦截用户的手机信息，接收手机验证码，被称为“拦截料”。在不少从事地下

交易的QQ群里，“拦截料”往往被明码标价出售。

“惊云”本身既向人出售钓鱼网站，自己也通过钓鱼网站获取他人的银行卡信息，并转手出售“拦截料”赚钱。

乌云网的白帽子黑客曾经就钓鱼网站发布报告，称钓鱼网站程序其实都很简单，重点是在界面的装修上，比如做成银行或运营商的样子。“这个链条中有专门的售卖团队，一套程序价格是几百块左右。提供程序的技术团队会给洗钱师保证一系列的技术服务，包括VPS服务器设置，网站建设甚至简单的系统安全防护”。

乌云网报告指出，为骗人而生的钓鱼网站本身也需要“系统安全防护”的原因是因为，钓鱼网站程序几乎全部存在“后门”，而如果有其他黑客通过这个“后门”同样获取了“鱼”的银行卡信息，就有可能把“拦截料”取走。很多钓鱼网站主人一天给伪基站“信使”发一万左右的工资，但取回来的“鱼”被别人盗走提前“洗”了，导致收益入不敷出。现在不少黑产从业者也在努力学习ASP程序的“后门”清理技术。

6月2日，中国银行业协会银行卡专业委员会发布了《中国银行卡产业发展蓝皮书（2017）》。报告称，通过攻击手机移动端，以欺诈手段盗取银行卡的风险明显提高。据公安部对部分省市的统计，涉及网络的银行卡犯罪案件，近年的年增长速度达到40%以上。

多种通道“洗料” “洗料人”与“料主”六四分成

在黑市中，银行卡信息被统称为“料”。其中，有验证码的“料”被称为“拦截料”，从博彩网站以黑客技术“拖库”出来的“料”叫做“菠菜料”，而通过POS机或者直接在ATM机上安装盗窃软件取得的料叫做“轨道料”。

不管从哪种途径“出料”，最后都需要借助一些“通道”把银行卡中的钱盗刷出来，这被称作“洗料”。

不管是伪基站也好，钓鱼网站也好，都是窃取用户银行卡信息的手段，但把银行卡中的钱“安全”提取出来，往往需要借助专业“洗料人”所掌握的“通道”。

“惊云”直言，最为“传统”的洗料通道是直接取现，这类“洗料人”被称为“取手团队”，具体手法是通过技术直接复制一张与银行卡原持有人一模一样的银行卡出来，然后找人直接去ATM机取款。“这些人总是最先被抓的，我曾经跟一个取手团队合作过，后来觉得太危险了就叫他们删除了我的联系方式。”

“现在，做通道的人都是金融行业从业者比较多，或者是熟悉金融行业的人士。因为从金融系统或者第三方支付平台上将钱‘划走’比较安全，风险也比较小。”“惊云”说。

6月8日，新京报记者以出料为名联系到一QQ名为“诚信为本”的专业“洗料人”。据他介绍，这一行的“行规”基本是开钓鱼网站的“料主”把出的“料”先提供给洗料人，洗料人通过自己的通道将银行卡里的钱提取出来，所获款项再与“料主”按一定比例分成，一般是隔天回款。

“诚信为本”表示他走的是“银行通道”，和“料主”按6：4分成。“我6你4，如果做得久了，老客户我们可以按照5：5分成。”他向新京报记者出示了一个显示时间为6月7日的招商银行的电子回单，“我们可以出四大行以及招行、浦发的储蓄卡，宗旨是一条料出到底，绝不跑单。”

但实际上，“料主”与“洗料人”之间常常发生“黑吃黑”，“料主”给了“洗料人”钱之后，“洗料人”独吞利润的案例也不鲜见。

6月8日，在一个从事黑料交易的QQ群中，一位“料主”与“洗料人”就发生了争执。“料主”称已把“料”发给了洗料人，但“洗料人”隔了三天都没回款。“洗料人”则喊冤称“钱还在，我根本没有洗这个料”。

“实际上，任何拥有手机短信权限，能通过银行卡卡号和密码进行转账操作的平台，都可以作为‘洗料’的通道，不同的是安全与否。”一位了解互联网黑产的人士告诉新京报记者。

该人士介绍，目前流行的“通道”包括开通快捷支付的各类网上银行系统，以及游戏币、卡盟话费或者其他第三方平台。

新京报记者查阅多份“信用卡诈骗”相关判决书后发现，在获得“料主”提供的银行卡信息后，“洗料人”可以利用上述信息骗取银行客服的信任，修改或增加被害人信用卡所绑定的手机号码，或者直接拦截被害人的手机短信。而“洗料人”在法院当庭供述的洗料“通道”包括支付宝、微信、易付宝、“去哪儿网”账户、“携程网”账户、电子加油卡账户等第三方支付平台。

难题：“盗刷很难判断泄露环节在哪里”

5月9日，最高人民法院与最高人民检察院联合发布《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》。《解释》明确，非法获取、出售或者提供公民个人信息违法所得五千元以上，即应当认定为刑法第二百五十三条之一规定的“情节严重”，可处三年以下有期徒刑或者拘役，并处或者单处罚金。

某安全公司技术专家向新京报记者表示，2017年第一季度拦截的垃圾短信中，有1100万条伪基站短信，占垃圾短信拦截总量的0.5%。一季度截获安卓平台新增恶意程序样本222.8万个，隐私窃取类木马占比7.9%。

专家称，2017年第一季度，伪基站短信在所有垃圾短信中的比例，相较于2016年第一季度（6.6%）、2016年全年（4%）有了明显下降。这说明通过公安机关、电信运营商、安全厂商等相关政府、企业联合打击治理后，伪基站短信得到了有效的治理。

21CN聚投诉在3月发布的银行卡盗刷大数据显示，2016年度，银行卡盗刷全网公开的投诉量共7095次，累计造成客户经济损失1.83亿元。2016年工商银行全年盗刷投诉量1923次，成为盗刷投诉第一大户，占总投诉量的25.6%，涉案金额3874.8万元。

北京盈科律师事务所方超强律师表示，一般用户银行卡信息泄露后遭到盗刷，很难判断泄露环节在哪里。但银行卡在盗刷时总会有IP地址显示，银行卡持有人只要证明银行卡被盗刷时的IP地址和本人当时所在地址不一致，就可以证明这单交易非本人操作，从而获得银行理赔。

“在实际维权过程中，如果银行卡持有人举证证明银行卡确实遭到盗刷，且过错是银行方面的漏洞，是可以获得银行赔偿的。不过在钓鱼网站泄露信息被盗刷的情况并不属于银行本身存在漏洞，只能说骗术过于高明，在这样的情况下，银行不需承担责任。”方超强表示。

6月8日，新京报记者拨打工商银行及招商银行客服咨询银行卡被盗刷之后可如何处理，工行客服回复称，如果用户账户遭到盗刷，可以立即申请拒付以避免更大损失；如果上了账户安全险，遭到盗刷后可以获取一定数额的赔偿，但并不能保证被盗刷走的钱一定能被追回来。招行则回复称具体处理情况需要根据盗刷者是境内境外盗刷以及线上还是线下盗刷来具体分析。

2016年，新京报曾经报道，受害者许先生在回复一条短信后，银行卡、支付宝、百度钱包内资金被盗走的情况。网络安全专家当时分析，这是一则利用“个人信息＋USIM卡＋改号软件发送诈骗短信”盗取资金的案件，在实施诈骗之前，骗子掌握了大量受害者的个人信息，包括姓名、手机号、身份证号、网银账户和密码，银行预留的验证手机号。不法分子获取个人信息主要的途径包括无良商家盗卖、网站数据窃取、木马病毒攻击、钓鱼网站诈骗、二手手机泄密和新型黑客技术窃取等。

第三方支付平台易联支付也遭遇过用户银行卡通过其平台被盗刷的情况。

5月4日，有用户反映自己银行卡上的500块钱被他人通过易联支付进入苹果账号充值“取走”。

易联支付相关负责人向新京报记者表示，该用户的银行卡在被盗刷过程中，均是在填写了正确的银行卡开户信息以及个人身份信息后，输入了正确的银行卡取款密码，易联支付通过银联及发卡行对支付信息进行校验后才成功扣款。“我们以此可以判断在银行卡被盗刷前，犯罪分子已经掌握了所有支付信息，包含银行卡取款密码。”

上述负责人表示，易联支付有“先行赔付”机制。“我们在收到该用户的投诉后，已第一时间联系商家冻结交易，并在投诉后的第1个工作日安排了退款。”

方超强表示，第三方平台属于支付的渠道和工具，在刷卡环节不认人，只和密钥比对，因此在银行卡盗刷事件中，第三方平台本身并不需要承担责任。

新京报记者 罗亦丹 陈鹏

转自搜狐，原文链接：http://www.sohu.com/a/147671677_470026。

专家点评

针对于银行卡盗刷事件，绿盟科技建议银行用户遵从以下建议：

1. 妥善保管银行卡和密码：盗刷行为发生的前提是盗刷人获取了银行卡信息和密码，持卡人作为银行卡和密码的保管主体，务必妥善谨慎保管，万不可出租、出借银行卡，不要将银行卡和密码交由他人使用，发现银行卡丢失或密码泄露后，及时办理挂失手续。

2. 用卡时注意环境的安全性：持卡人应当提高安全防范意识，在使用银行卡时注意ATM机或POS机周围有无可疑设备；排队办理银行卡业务时注意与他人保持安全距离，防止密码被窥视；进行网上支付操作时注意网址是否正确，网页是否存在异常链接等。

3. 妥善保管绑定银行卡的手机：手机与银行业务的联合使得手机不再是简单的通讯工具，具有了更强的财产属性和隐私性，持卡人务必妥善保管手机。

4. 设定账户变动短信提示：短信提示能够让持卡人及时发现账户异常变动情况，及时采取应对措施。

5. 不在公共WIFI下进行网上支付：随着公共WIFI覆盖范围的扩大和网上购物的兴起，购物突破了时间和空间的限制。但是，在公共WIFI下进行网上支付存在安全隐患，容易导致银行卡信息和密码泄露。

NSFOCUS

漏洞聚焦

EternalRocks(永恒之石) 技术分析与防护方案

发布时间：2017 年 5 月 25 日

1. 综述

继“永恒之蓝”勒索病毒后，近日，我们发现了最新病毒“永恒之石”（EternalRocks）。该病毒属于网络蠕虫，具有自我复制的功能，并利用MS17-010漏洞进行传播。与WannaCry不同，“永恒之石”利用更多近期泄露的NSA黑客工具，其中包括多种漏洞攻击工具。

参考链接：https://threatpost.com/eternalrocks-worm-spreads-seven-nsa-smb-exploits/125825/?utm_source=tuicool&utm_medium=referral

https://github.com/stamparm/EternalRocks

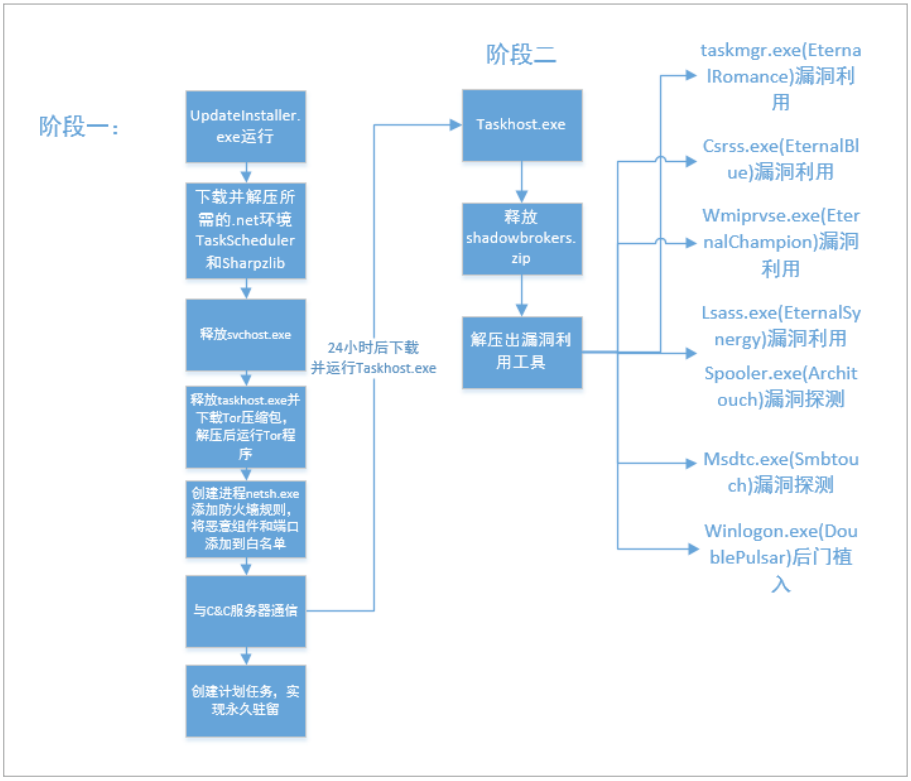
2. 文件结构

文件名	MD5	功能
UpdateInstaller.exe	496131B90F**********D2DD21213646	下载所需的 .net 环境，释放 svchost.exe
svchost.exe	5C9F450F24**********A0BD37DB6A40	释放 taskhost.exe。下载 Tor 并运行
Taskhost.exe	C52F20A85**********1248FD84AAA95	释放漏洞利用工具，扫描随机 IP，调用后续程序利用漏洞进行攻击
taskmgr.exe	4420F89**********D2EF14136032F69	漏洞利用工具
csrss.exe	8C80DD**********7C1E549CB59BCBF3	漏洞利用工具
wmiprvse.exe	D2FB0**********4FBD1B18E475C9F23	漏洞利用工具
lsass.exe	2A8D4**********482750FE052223C3D	漏洞利用工具
spooler.exe	30380B**********006216F33FA06964D	漏洞探测工具
msdtc.exe	B50FF**********29A00B245E4D0C863	漏洞探测工具
winlogon.exe	C243**********2110977DACAFE6C8C1	后门植入工具

3. 攻击目标

含有MS17-010漏洞的计算机。

4. 攻击流程

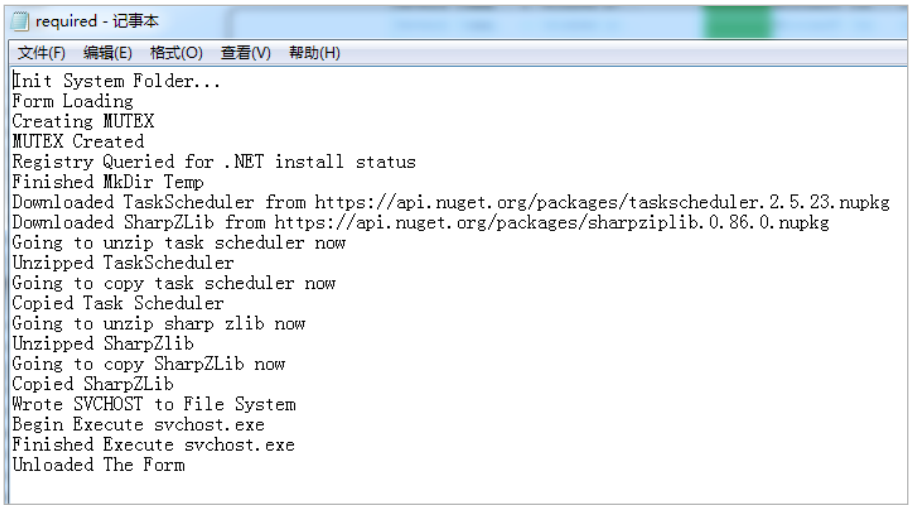


5. 样本分析

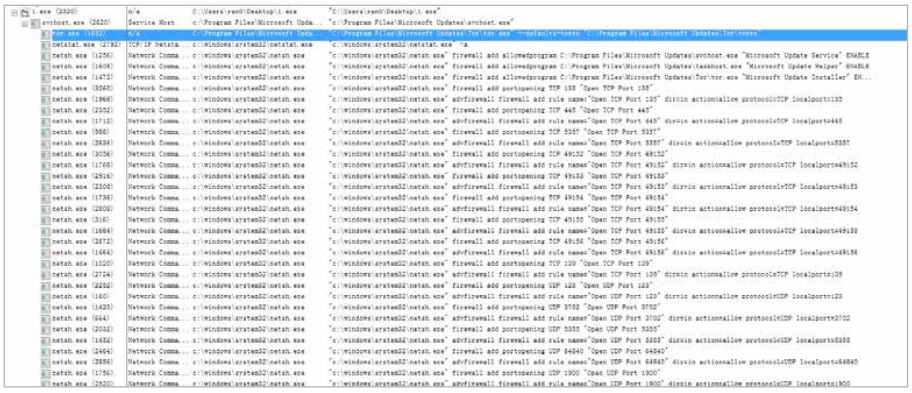
EternalRocks病毒文件是通过MS17-010漏洞进行传播的，我们将以其在目标机的执行流程为线，介绍其攻击过程及其功能。

5.1 阶段一：UpdateInstaller.exe

第一阶段的样本UpdateInstaller.exe创建目录C:\Program Files\Microsoft Updates，下载并解压必须的.NET组件（提供给之后的阶段使用）TaskScheduler和SharpZlib，下载完之后会释放svchost.exe并运行。可以从样本记录的日志中看出它的行为。



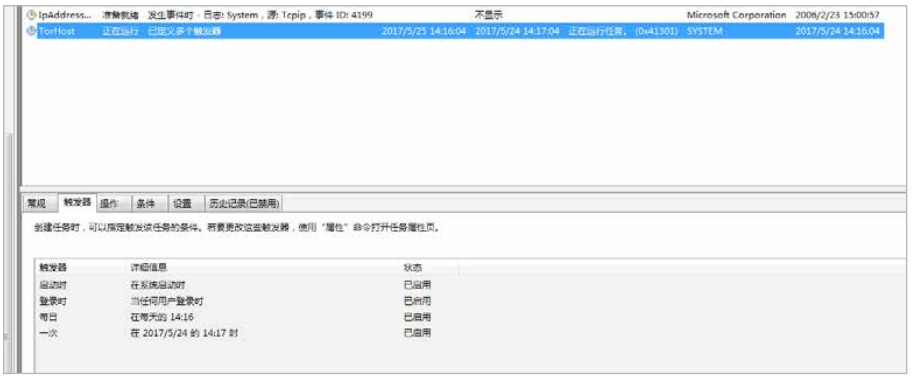
svchost.exe会释放taskhost.exe，然后从archive.torproject.org下载Tor压缩包，解压缩后运行Tor程序，然后通过创建进程netsh.exe附加参数的方式添加防火墙规则，将病毒攻击组件（C:\Program Files\Microsoft Updates\svchost.exe、C:\Program Files\Microsoft Updates\taskhost.exe）、Tor组件（C:\Program Files\Microsoft Updates\Tor\tor.exe）、端口加入白名单，启用防火墙后退出(添加规则的具体命令放在附录部分)。



与C&C服务器 f3sxk2g3evjr7di5.onion（f3sxk2g3evjr7di5每次获取的都不一

样，存放在C:\Program Files\Microsoft Updates\Tor\hidden_service\ hostname文件中）进行通信。

创建计划任务



感染24小时后，样本会在http:// f3sxk2g3evjr7di5.onion/updates/download?id=PC站点下载恶意程序taskhost.exe（与第一阶段的病毒文件不同）。

5.2 阶段二：EternalRocks

此阶段需要使用的样本Taskhost.exe，使用dnspy载入后，可以看到原名为EternalRocks。

```
[assembly: AssemblyVersion("1.0.0.0")]
[assembly: Debuggable(DebuggableAttribute.DebuggingModes.Default |
[assembly: AssemblyCompany("Microsoft")]
[assembly: AssemblyConfiguration("")]
[assembly: AssemblyCopyright("Copyright © Microsoft 2017")]
[assembly: AssemblyDescription("")]
[assembly: AssemblyFileVersion("1.0.0.0")]
[assembly: AssemblyProduct("EternalRocks")]
[assembly: AssemblyTitle("EternalRocks")]
[assembly: AssemblyTrademark("")]
[assembly: CompilationRelaxations(8)]
[assembly: RuntimeCompatibility(WrapNonExceptionThrows = true)]
[assembly: ComVisible(false)]
[assembly: Guid("3f701d4b-9b5d-40f1-bb00-40757ddc1634")]
```

运行Taskhost.exe后，它会在当前目录下释放并解压shadowbrokers.zip。

bins	2017/5/24 10:45	文件夹	
configs	2017/5/24 10:45	文件夹	
payloads	2017/5/24 10:45	文件夹	
SharpZLib	2017/5/24 10:18	文件夹	
TaskScheduler	2017/5/24 10:18	文件夹	
temp	2017/5/24 17:25	文件夹	
ICSharpCode.SharpZipLib.dll	2011/1/3 14:16	应用程序扩展	196 KB
installed.ete	2017/5/24 10:45	ETE 文件	1 KB
Microsoft.Win32.TaskScheduler.dll	2017/4/7 17:06	应用程序扩展	341 KB
required.glo	2017/5/24 10:18	GLO 文件	1 KB
shadowbrokers.zip	2017/5/24 10:45	好压 ZIP 压缩文件	4,258 KB
SharpZLib.zip	2017/5/24 10:18	好压 ZIP 压缩文件	444 KB
startup.fixed	2017/5/24 10:45	FIXED 文件	1 KB
svchost.exe	2017/5/24 10:18	应用程序	297 KB
Taskhost.exe	2017/5/22 0:54	应用程序	5,152 KB
TaskScheduler.zip	2017/5/24 10:18	好压 ZIP 压缩文件	870 KB
UpdateInstaller.exe	2017/5/22 0:54	应用程序	332 KB

释放的这些文件中主要就是漏洞相关程序，包含漏洞利用，漏洞扫描和后门植入程序。之后，Taskhost.exe将会随机扫描IP地址并发送syn数据包等待回链，如果对方没有回传ack包就尝试连接下一个IP地址，一旦和目标IP连接成功，便启动bin目录下的进程msdtc.exe（Smbtouch.exe）进行漏洞探测，一旦探测到有可用的漏洞，就利用后门植入程序将第一阶段的UpdateInstall.exe植入到目标机器中。

6. 网络规则

样本与以下链接产生通信：

1. 下载.net组件:

https://api.nuget.org/packages/taskscheduler.2.5.23.nupkg

https://api.nuget.org/packages/sharpziplib.0.86.0.nupkg

2. 下载tor

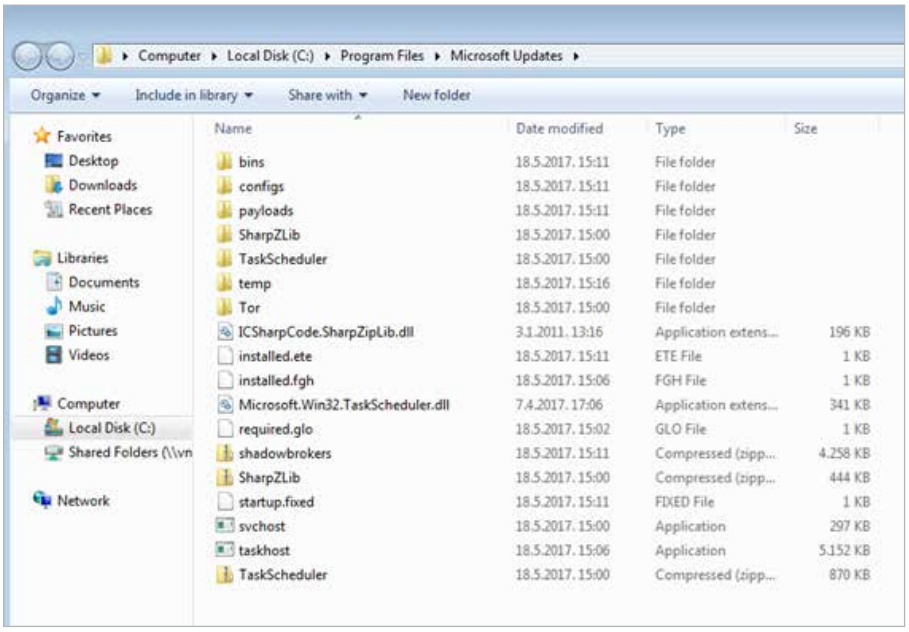
https://archive.torproject.org

7. 检测与防护方案

检测

1. 本地检查

病毒感染主机后，会创建C:\Program Files\Microsoft Updates\目录，生成多个病毒文件，如下图：

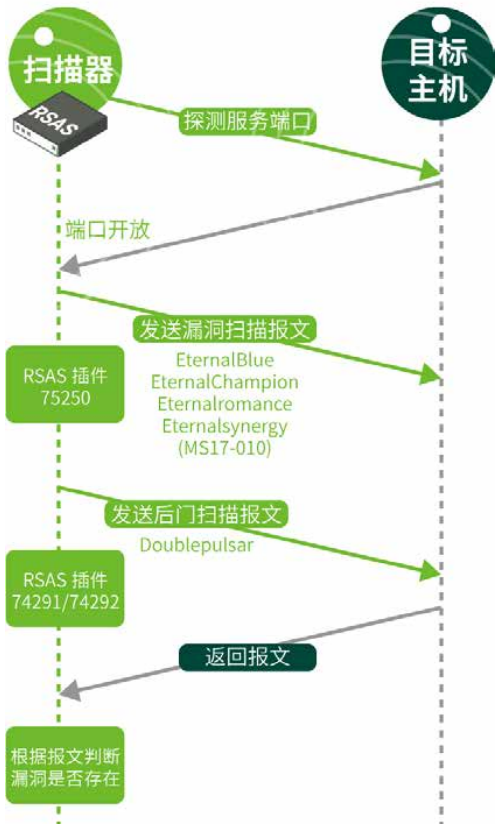


进入开始菜单—控制面板—管理工具—计划任务，展开任务计划程序库—Microsoft—Windows，病毒会创建2个计划任务ServiceHost和TaskHost，如下图：

在主机上发现以上特征，即可判断已经感染EternalRocks病毒。

2. 远程扫描

管理员可使用绿盟极光远程安全评估系统RSAS对网络内未安装补丁及中了Doublepulsar后门的主机进行远程检测，如下图：



隔离

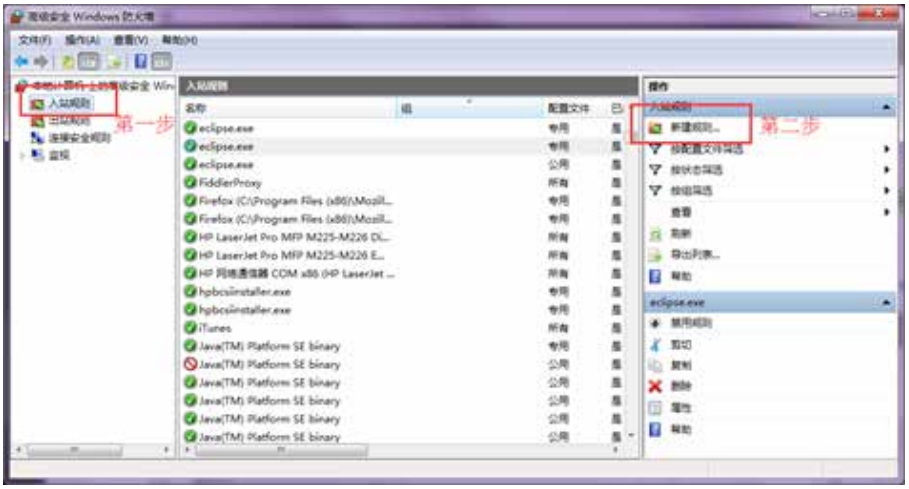
◆ 断网

检测阶段发现的已感染病毒的主机应立即进行断网，避免病毒进一步在网络内扩散。

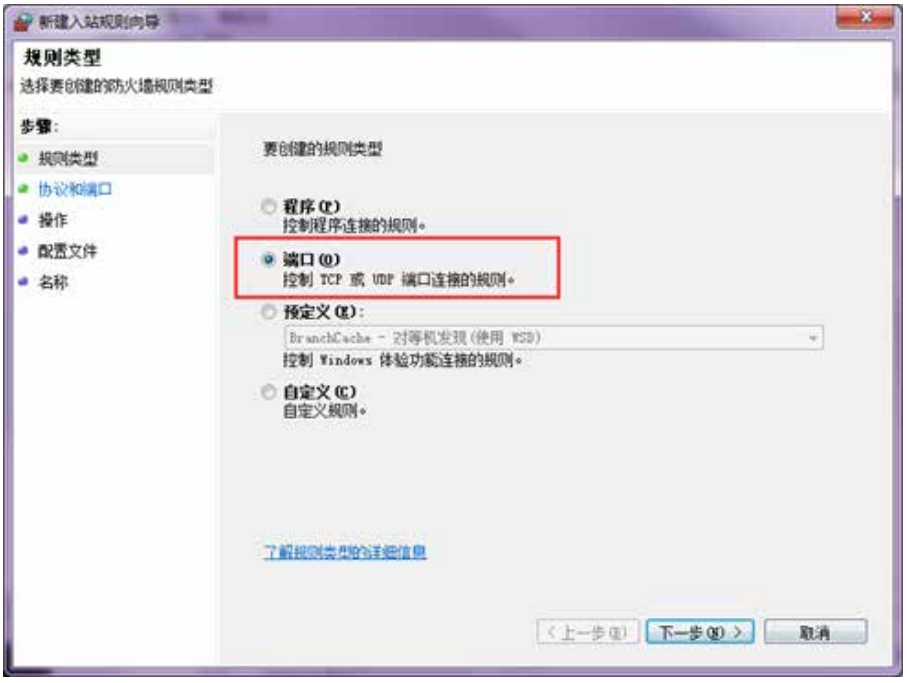
◆ 封锁端口

对于未安装MS17-010补丁的和存在Doublepulsar后门的主机，应立即封锁Windows SMB服务TCP 445端口，方法如下：

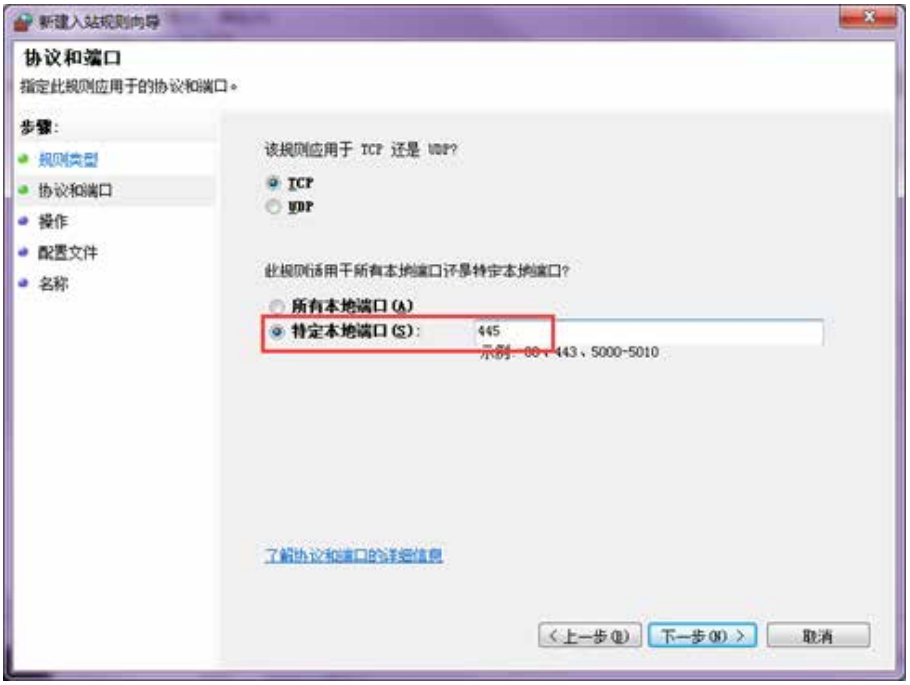
1. 开始—控制面板—Window防火墙，点击左侧高级设置，点击左侧入站规则，再点击右侧新建规则创建防火墙入站规则：



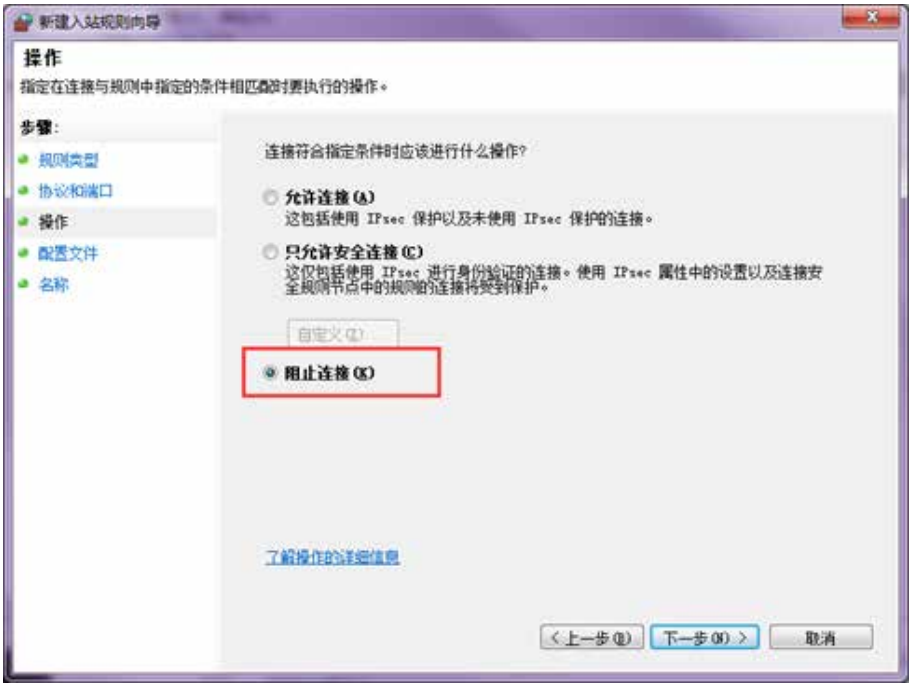
2. 在新建入站规则向导中，针对协议和端口步骤，选择对端口过滤。



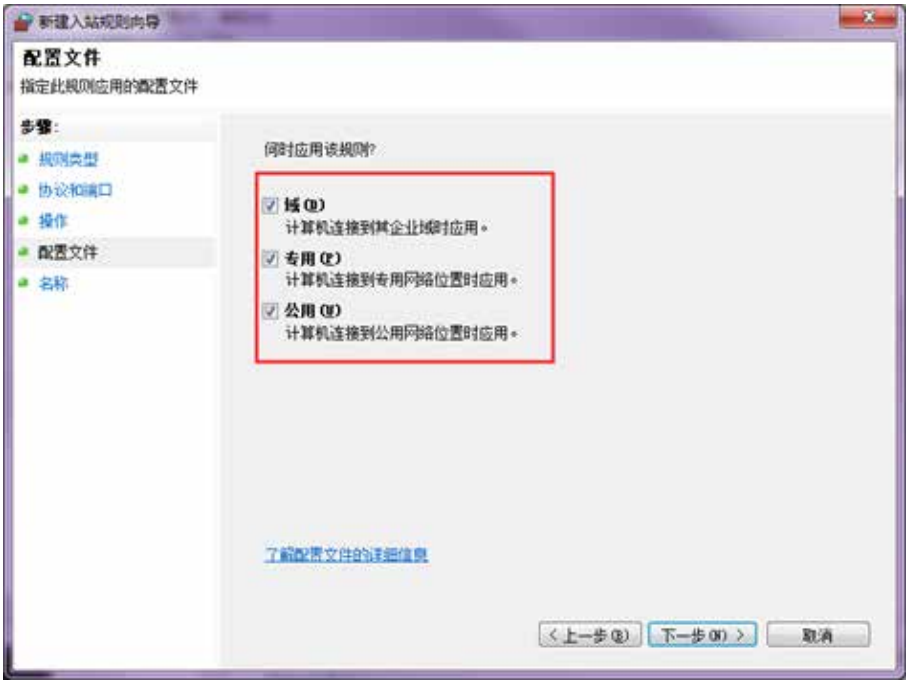
3. 选择TCP协议和特定本地端口：445



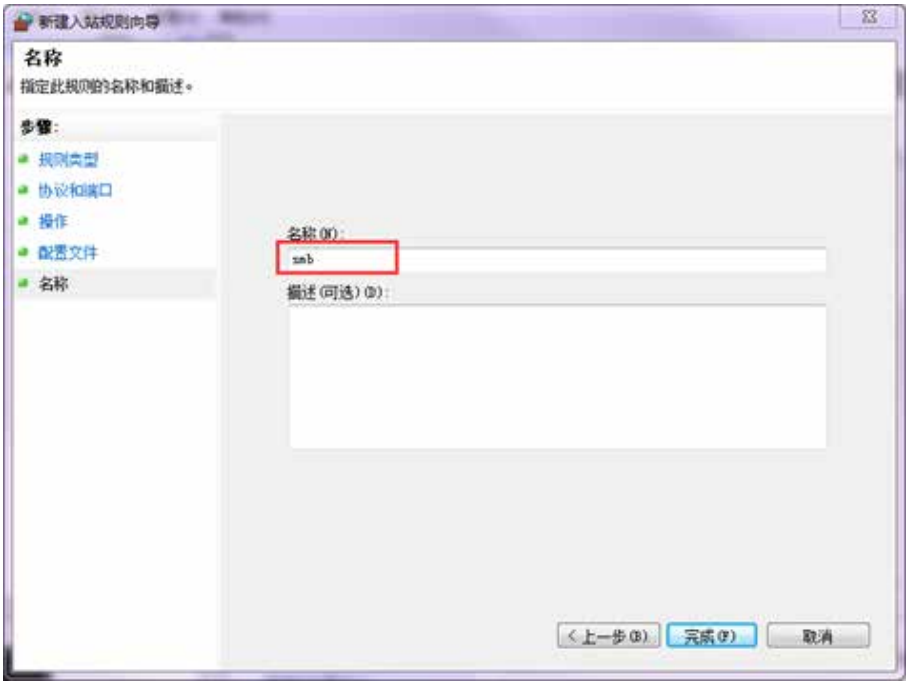
4. 在操作步骤中，选择阻止连接。



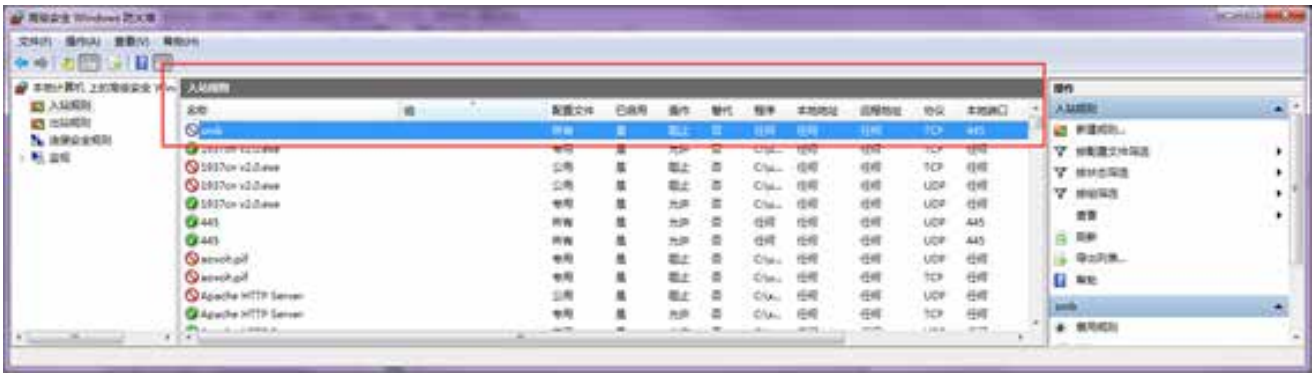
5. 在应用该规则处，勾选域、专用以及公用选项。



6. 填入规则名称，完成创建。

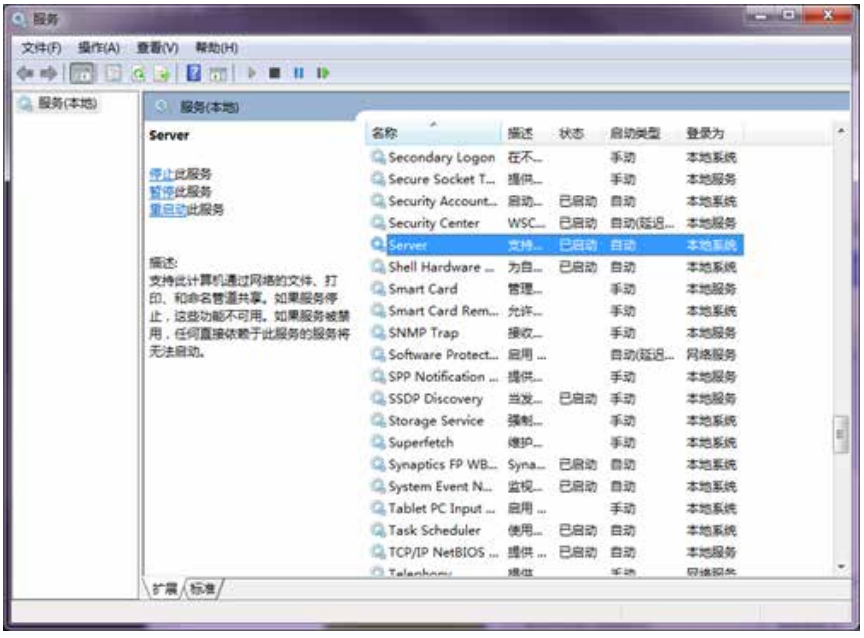


7. 规则创建完成后，可看到入站规则中存在445阻断规则。

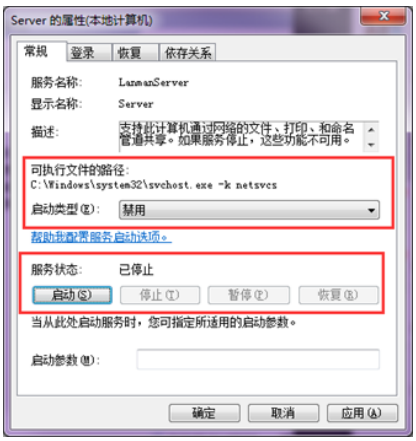


除使用Windows防火墙封锁TCP 445端口外，还可以直接禁用Server服务，如下：

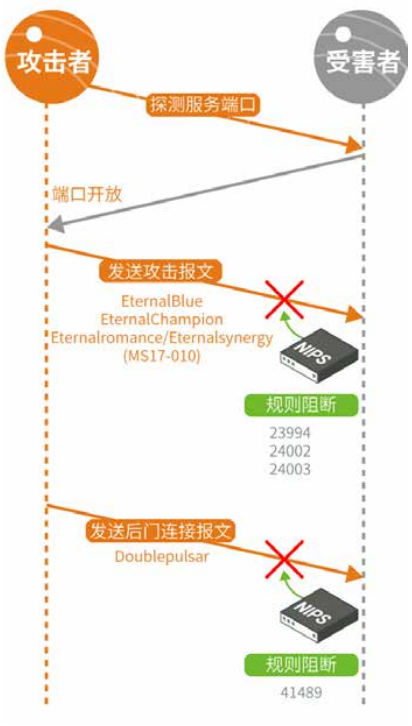
1. 点击开始菜单—运行，输入msc，进入服务管理器，找到server服务。



2．双击将启动类型修改为禁用，点击停止按钮，将服务状态修改为已停止。



重新启动主机即可彻底关闭TCP 445端口。



修复

◆ 清除病毒

1. 进入开始菜单—控制面板—管理工具—计划任务，展开任务计划程序库—Microsoft—Windows，删除计划任务ServiceHost和TaskHost。

2. 停止以下进程：

C:\Program Files\Microsoft Updates\svchost.exe

C:\Program Files\Microsoft Updates\taskhost.exe

C:\Program Files\Microsoft Updates\torunzip.exe

3. 删除C:\Program Files\Microsoft Updates\目录及其中所有文件。

4. 安装补丁

下载并安装微软官方补丁：

https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx

监测

◆ 网络监测和阻断

管理员可使用绿盟入侵防御系统NIPS对网络中的攻击报文和Doublepulsar后门连接报文进行阻断，防范病毒进一步扩散，如左图：

同时也可使用此方法监测网络中是否有病毒扩散，帮助管理员定位感染病毒的主机。

8. 总结

通过分析可知，此恶意程序利用的依然是先前ShadowBrokers爆出的漏洞。虽然此次事件掀起了轩然大波，各大安全厂商也都提供了防御措施，但是还是有用户没有针对此次事件进行相关的补救措施。为了防止后续其他人利用此漏洞进行攻击，建议尽快采取相应的防御措施，以免造成损失。

Linux 多个内核拒绝服务漏洞安全威胁通告

CVE-2017-8890
CVE-2017-9075
CVE-2017-9076
CVE-2017-9077

发布时间：2017 年 6 月 16 日

综述

近日， Linux内核存在的多个拒绝服务漏洞被公布，涉及CVE-2017-8890、CVE-2017-9075、CVE-2017-9076、CVE-2017-9077，影响几乎所有Linux kernel 2.5.69 ~Linux kernel 4.11的内核版本。

各CVE描述如下：

CVE 编号	漏洞描述	漏洞影响	是否远程
CVE-2017-8890	Linux 内 核 中 net / ipv4 / inet_connection_sock.c 中的 inet_csk_clone_lock 函数存在内存 2 次释放漏洞	在组播模式下，可能导致远程拒绝服务或远程代码执行	远程（需要开启组播模式）
CVE-2017-9075	Linux 内核中的 net / sctp / ipv6.c 中的 sctp_v6_create_accept_sk 函数处理不当	内核崩溃，拒绝服务。	本地
CVE-2017-9076	Linux 内核中的 net / dccp / ipv6.c 中的 dccp_v6_request_recv_sock 函数处理不当	内核崩溃，拒绝服务。	本地
CVE-2017-9077	Linux 内 核 中 的 net / ipv6 / tcp_ipv6.c 中 的 tcp_v6_syn_recv_sock 函数处理不当	内核崩溃，拒绝服务。	本地

注：对于CVE-2017-8890，要主机可以接收组播报文才有可能被远程利用导致拒绝服务。组播功能的使用需要在交换机上开启组播模式，此模式在交换机上是默认关闭的。

受影响的版本

目前几乎所有的Linux内核版本（2.5.69 - 4.11）及其对应的发行版本应该都受影响。

目前确认的受影响版本的详细列表请参照文末附录。

不受影响的版本

- ☐ Linux 4.12-rc1 (非正式版)
- ☐ Linux 4.12-rc2 (非正式版)
- ☐ Linux 4.12-rc3 (非正式版)
- ☐ Linux 4.12-rc4 (非正式版)
- ☐ Linux 4.12-rc5 (非正式版)

规避方案

1. 官方已经进行了代码修复，用户可自行参照如下地址进行代码修改，重新编译和启用新内核来修复漏洞。

☐ CVE-2017-8890:

http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=657831ffc38e30092a2d5f03d385d710eb88b09a

☐ CVE-2017-9075：

http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=fdcee2cbb8438702ea1b328fb6e0ac5e9a40c7f8

☐ CVE-2017-9076:

http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=83eaddab4378db256d00d295bda6ca997cd13a52

☐ CVE-2017-9077:

http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=83eaddab4378db256d00d295bda6ca997cd13a52

2. 在非必要的情况下，请关闭三层交换机的组播模式。

3. 使用 Grsecurity/PaX 对内核加固.

Microsoft Windows 6 月份安全补丁修复严重漏洞安全威胁通告

发布时间：2017 年 6 月 14 日

综述

近日，微软发布的6月份安全更新补丁修复了十余个关键漏洞，其中包含了2个被利用的重大远程代码执行漏洞：Windows Search远程代码执行漏洞（CVE-2017-8543）以及LINK文件快捷方式远程代码执行漏洞（CVE-2017-8464）。

用户应立即启动自动更新服务，下载并安装此次安全补丁来防护相关漏洞。对于已经不再受官方支持的系统版本，此次微软也发布了对应的补丁，用户可以手动下载安装该补丁来防护相关漏洞。

相关地址：

https://threatpost.com/microsoft-patches-two-critical-vulnerabilities-under-attack/126239/

https://technet.microsoft.com/en-us/library/security/4025685.aspx

https://blogs.technet.microsoft.com/msrc/2017/06/13/june-2017-security-update-release/

漏洞概述

Windows Search服务远程代码执行漏洞

CVE编号：CVE-2017-8543

当Windows Search处理内存中的对象时，存在远程执行代码漏洞。 成功利用此漏洞的攻击者可以控制受影响的系统。 攻击者可以安装程序; 查看，更改或删除数据; 或创建具有完全用户权限的新帐户。

为了利用此漏洞，攻击者可以向Windows Search服务发送特制的SMB消息。 访问目标计算机的攻击者可以利用此漏洞提升权限并控制计算机。 此外，在企业场景中，远程未经身份验证的攻击者可以通过SMB连接远程触发漏洞，然后控制目标计算机。

参考链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8543

Windows LINK文件远程代码执行漏洞

CVE编号: CVE-2017-8464

Microsoft Windows中存在远程代码执行漏洞，如果处理了.LNK文件，则可能允许远程执行代码。

成功利用此漏洞的攻击者可以获得与本地用户相同的用户权限。 其帐户被配置为具有较少用户权限的系统的用户可能比使用管理用户权限的用户受到的影响更小。

攻击者可以向用户呈现包含恶意的.LNK文件和相关联的恶意二进制文件的可移动驱动器或远程共享。 当用户在Windows资源管理器或解析.LNK文件的任何其他应用程序中打开此驱动器（或远程共享）时，恶意二进制程序将在目标系统上执行攻击者选择的代码。

参考链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8464

其余漏洞信息，请参考微软官方说明：https://technet.microsoft.com/en-us/library/security/4025685.aspx

受影响的版本

- ☐ Windows 10
- ☐ Windows 7
- ☐ Windows 8.1
- ☐ Windows 8
- ☐ Windows Vista
- ☐ Windows RT 8.1
- ☐ Windows Server 2016
- ☐ Windows Server 2012
- ☐ Windows Server 2008

受影响版本的详细信息，请参考微软官方说明链接：

Windows Search服务远程代码执行漏洞：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8543

Windows LINK 远程代码执行漏洞：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8464

解决方案

微软官方已经在6月份发布的安全补丁中修复了包括上述2个严重漏洞在内的十余个重大安全漏洞，受影响的用户应立即通过Windows自动更新服务来下载更新该安全补丁来防护。

参考链接：

https://support.microsoft.com/zh-cn/help/4025686/microsoft-security-advisory-4025685-guidance-for-supported-platforms

对于不受支持的旧版本，微软官方也发布了对应的补丁，用户可以通过手动下载安装该补丁来进行防护。

参考链接：https://support.microsoft.com/zh-cn/help/4025687/microsoft-security-advisory-4025685-guidance-for-older-platforms

暗云 III 木马程序安全威胁通告

发布时间：2017 年 6 月 15 日

综述

近日，一款名为暗云III的木马被发现在网络上有大面积的攻击行为，该木马通过下载站点大规模传播，随后会感染磁盘MBR来实现开机自动，大量用户被检测到受感染。

攻击者可以将受感染的用户可以作为僵尸网络来进行分布式拒绝服务攻击（DDoS），劫持流量来牟利等。

参考链接：

http://www.freebuf.com/articles/system/134017.html

https://www.leiphone.com/news/201706/7pcuo6TVrAJO5UY4.html

木马行为概述

攻击者通过patch正常的游戏微端将shellcode捆绑到正常的程序中来进行推广传播。通过不同的patch代码，不同的shellcode将会被执行，包括替换原本加载的资源并调用新的shellcode来加载PE文件，该PE文件会对各种条件进行判断，只有符合条件才会下载暗云III的感染程序到本地。这些条件包括检测是否为虚拟机，是否位于网吧，是否检测到杀毒软件等。在满足这些条件后，暗云程序会感染并修改MBR，实现在系统中潜伏并在系统每次运行时调用其内的另一shellcode。该shellcode会随后下

载更多的模块以及配置文件，攻击者可以通过配置文件对感染的主机发布指令。

建议方案

1. 用户行为

◆ 用户应该提高上网安全意识，在官方站点下载应用软件，以免下载到被木马感染的软件。

◆ 定期备份重要的文件及数据，保证敏感信息的安全。

2. 终端防护产品

用户应该在本地主机上安装终端防护产品，如金山V8+ 企业安全终端，及时发现与查杀恶意软件。

3. 软件检测

在未安装终端防护软件的情况下，针对从网络下载下来的不明软件可以通过NSFOCUS 威胁分析中心（https://poma.nsfocus.com/）进行信誉分析或者提交TAC产品进行安全监测。

4. 服务类

◆ 短期服务：绿盟科技工程师现场木马后门清理服务。确保第一时间消除网络内相关风险点，控制事件影响范围，提供事件分析报告。

◆ 中期服务：提供3-6个月的风险监控与巡检服务（IPS+TAC+人工服务）。长期对此恶意样本进行检测，保护客户系统安全。

◆ 长期服务：基于行业业务风险解决方案（威胁情报+攻击溯源+专业安全服务）

多个 Apache httpd 安全漏洞安全威胁通告

发布时间：2017 年 6 月 21 日

综述

近日，Apache 官方发布了httpd的新版本修复了多个安全漏洞，涉及CVE-2017-3167，CVE-2017-3169，CVE-2017-7659，CVE-2017-7668，CVE-2017-7679，可以造成身份验证被绕过以及拒绝服务攻击等。大部分Apache httpd 2.2.x以及2.4.x版本均受影响。相关漏洞信息如下：

CVE 编号	漏洞描述
CVE-2017-3167	第三方模块在验证阶段以外调用 ap_get_basic_auth_pw() 时 有可能导致验证要求被绕过
CVE-2017-3169	当第三方模块在调用 ap_hook_process_connection() 发 送 HTTP 请求给 HTTPS 端口时，mod_ssl 可能会间接引用空指针
CVE-2017-7659	在处理恶意构造的 HTTP/2 请求时，mod_http2 可能会间接引用空指针，使服务器进程崩溃
CVE-2017-7668	HTTP 严格解析改动中存在一个令牌列表解析的 BUG，ap_find_token() 可以搜索输入字符串之外的内容。通过构造一个恶意的请求头，攻击者可以造成段错误或者强行让 ap_find_token() 返回一个错误的值
CVE-2017-7679	当攻击者发送一个恶意的 Content-Type 响应头时，mod_mime 会越界读取缓冲区内容。

参考链接：

https://httpd.apache.org/security/vulnerabilities_24.html

https://httpd.apache.org/security/vulnerabilities_22.html

受影响的版本

- ☐ Apache httpd 2.2.x < 2.2.33-dev
- ☐ Apache httpd 2.4.x < 2.4.26

各漏洞影响的版本详细信息可参考文末附录。

不受影响的版本

- ☐ Apache httpd 2.2.33-dev
- ☐ Apache httpd 2.4.26

规避方案

Apache 官方已经针对2.2.x以及2.4.x发布了相应的2.2.33-dev以及2.4.26新版本修复了上述各漏洞，请受影响的用户及时下载更新至最新版本来防护漏洞。请参考如下连接：

2.2.x版本：https://httpd.apache.org/security/vulnerabilities_22.html

2.4.x版本：https://httpd.apache.org/security/vulnerabilities_24.html

附录

各漏洞影响版本的具体信息如下：

CVE-2017-3167

2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.32, 2.2.31, 2.2.29, 2.2.27, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

CVE-2017-3169

2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.32, 2.2.31, 2.2.29, 2.2.27, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

CVE-2017-7659

2.4.25

CVE-2017-7668

2.4.25, 2.2.32

CVE-2017-7679

2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.32, 2.2.31, 2.2.29, 2.2.27, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

使用硬件加速的勒索软件——XData

发布时间：2017年5月27日

概述

近日，一款名为Xdata的勒索软件大范围攻击了乌克兰的计算机设备，被攻击的主机上文件被加密，攻击者要求通过匿名邮件联系，来支付赎金并且获得解密的方法。

该勒索软件通过判断受害主机是否支持AES-NI指令集，若支持，则采用硬件加速加密文件过程。

AES-NI指令集

高级加密标准新指令（Advanced Encryption Standard New Instructions; AES-NI），是一个x86指令集架构的扩展，用于Intel和AMD微处理器，由Intel在2008年3月提出。该指令集的目的是改进应用程序使用高级加密标准（AES）执行加密和解密的速度。

AES-NI新指令如下表所示：

指令	描述
AESENC	执行一轮 AES 加密流
AESENCLAST	执行最后一轮 AES 加密流
AESDEC	执行一轮 AES 解密流
AESDECLAST	执行最后一轮 AES 解密流
AESKEYGENASSIST	协助生成 AES 轮回秘钥
AESIMC	协助 AES 逆列混合

AESENC，AESENCLAST，AESDEC，AESDECLAST四条指令完成加解密功能，每条指令有两个参数register-register或register-memory。

AESENC完成一轮加密操作，包括四步：

- 字节替代（SubBytes）

- 行移位（ShiftRows）
- 列混淆（MixColumns）
- 轮密钥加（AddRoundKey）

AESENCLAST完成最后一轮加密操作：

- 字节替代（SubBytes）
- 行移位（ShiftRows）
- 轮密钥加（AddRoundKey）

AESDEC完成一轮解密操作，包括四步：

- 逆向字节替代（InvSubBytes）
- 逆向行移位（InvShiftRows）
- 逆向列混淆（InvMixColumns）
- 轮密钥加（AddRoundKey）

AESDECLAST完成最后一轮解密操作：

- 逆向字节替代（InvSubBytes）
- 逆向行移位（InvShiftRows）
- 和轮密钥加（AddRoundKey）

AESENC和AESENCLAST加密操作伪代码如下：

```
AESENC xmm1, xmm2/m128                  AESENCLAST xmm1, xmm2/m128
Tmp := xmm1                             Tmp := xmm1
Round Key := xmm2/m128                  Round Key := xmm2/m128
Tmp := ShiftRows (Tmp)                  Tmp := Shift Rows (Tmp)
Tmp := SubBytes (Tmp)                   Tmp := SubBytes (Tmp)
Tmp := MixColumns (Tmp)
xmm1 := Tmp xor Round Key               xmm1 := Tmp xor Round Key
```

AESDEC和AESDECLAST解密操作伪代码如下：

```
AESDEC xmm1, xmm2/m128                  AESDECLAST xmm1, xmm2/m128
Tmp := xmm1                             State  := xmm1
Round Key := xmm2/m128                  Round Key  := xmm2/m128
Tmp := InvShift Rows (Tmp)              Tmp := InvShift Rows (State)
Tmp := InvSubBytes (Tmp)                Tmp := InvSubBytes (Tmp)
Tmp := InvMixColumns (Tmp)
xmm1 := Tmp xor Round Key               xmm1:=  Tmp xor Round Key
```

AES-128加密过程如下：

```
; AES-128 encryption sequence.
; The data block is in xmm15.
; Registers xmm0-xmm10 hold the round keys(from 0 to 10 in this order).
; In the end, xmm15 holds the encryption result.
        pxor xmm15, xmm0                ; Whitening step (Round 0)
        aesenc xmm15, xmm1              ; Round 1
        aesenc xmm15, xmm2              ; Round 2
        aesenc xmm15, xmm3              ; Round 3
        aesenc xmm15, xmm4              ; Round 4
        aesenc xmm15, xmm5              ; Round 5
        aesenc xmm15, xmm6              ; Round 6
        aesenc xmm15, xmm7              ; Round 7
        aesenc xmm15, xmm8              ; Round 8
        aesenc xmm15, xmm9              ; Round 9
        aesenclast xmm15, xmm10         ; Round 10
```

AES-192解密过程如下：

```
; AES-192 decryption sequence.
; The data is in xmm15.
; Registers xmm12 - xmm0 hold the decryption round keys.
; (the decryption round keys are derived from the encryption round keys by
; passing them (except for the first and the last) through the
; InvMixColumns transformation.)
; In the end - xmm15 holds the decryption result
        pxor xmm15, xmm12               ; First xor
        aesdec xmm15, xmm11             ; Round 1 (consuming round keys in reverse order)
        aesdec xmm15, xmm10             ; Round 2
        aesdec xmm15, xmm9              ; Round 3
        aesdec xmm15, xmm8              ; Round 4
        aesdec xmm15, xmm7              ; Round 5
        aesdec xmm15, xmm6              ; Round 6
        aesdec xmm15, xmm5              ; Round 7
        aesdec xmm15, xmm4              ; Round 8
        aesdec xmm15, xmm3              ; Round 9
        aesdec xmm15, xmm2              ; Round 10
        aesdec xmm15, xmm1              ; Round 11
        aesdeclast xmm15, xmm0          ; Round 12
```

AESKEYGENASSIST和AESIMC两条指令是加解密操作的扩展指令，AESKEYGENASSIST用于协助生成AES轮回秘钥，AESIMC用于协助解密操作AES逆列混合。

AESKEYGENASSIST指令操作伪代码：

```
AESKEYGENASSIST xmm1, xmm2/m128, imm8
Tmp := xmm2/LOAD(m128)
X3[31-0] := Tmp[127-96];
X2[31-0] := Tmp[95-64];
X1[31-0] := Tmp[63-32];
X0[31-0] := Tmp[31-0];
RCON[7-0] := imm8;
RCON [31-8] := 0;
xmm1 := [RotWord (SubWord (X3)) XOR RCON, SubWord (X3),
                    RotWord (SubWord (X1)) XOR RCON, SubWord (X1)]
```

AESIMC指令操作伪代码如下：

```
AESIMC xmm1, xmm2/m128
RoundKey := xmm2/m128;
xmm1 := InvMixColumns (RoundKey)
```

参考链接：

https://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni

https://software.intel.com/en-us/articles/intel-advanced-encryption-standard-aes-instructions-set

Xdata勒索软件AES-NI使用

Xdata勒索软件通过判断受害主机是否支持AES-NI指令集，若支持，则采用硬件加速加密文件过程：

```
if ( dword_411BA0 )
{
  sub_40DFE0(v18, v18, (int)&v37, v17 >> 4);// aes-ni加密
}
else                                    // 非硬件加速
{
  v20 = (_DWORD *)v18;
  if ( v17 )
  {
    v21 = 0;
    do
    {
      sub_404730(v20, (int)v20, (int)&v42);
      v21 += 16;
      v20 += 4;
    }
    while ( v21 < v17 );
    v19 = v29;
  }
  v15 = v28;
}
v38 += v17;
if ( v31 )
  ((void (__stdcall *)(int, unsigned int))(dword_412228 ^ dword_4110A4))(v19, v17);
((void (__stdcall *)(int))(dword_41220C ^ dword_4110A4))(v19);
v14 = v25;
v15 += 10485760;
v28 = v15;
```

使用aeskeygenassist指令协助生成AES轮回秘钥:

```
.text:00401638                  movdqu  xmm1, xmmword ptr [ecx]
.text:0040163C                  movdqu  xmm3, xmmword ptr [ecx+10h]
.text:00401641                  movdqu  xmmword ptr [edx], xmm1
.text:00401645                  movdqu  xmmword ptr [edx+10h], xmm3
.text:0040164A                  add     edx, 20h
.text:0040164D                  movdqa  xmm5, xmmword_411010
.text:00401655                  aeskeygenassist xmm2, xmm3, 1
.text:0040165B                  call    sub_401030
.text:00401660                  aeskeygenassist xmm2, xmm3, 2
.text:00401666                  call    sub_401030
.text:0040166B                  aeskeygenassist xmm2, xmm3, 4
.text:00401671                  call    sub_401030
.text:00401676                  aeskeygenassist xmm2, xmm3, 8
.text:0040167C                  call    sub_401030
.text:00401681                  aeskeygenassist xmm2, xmm3, 10h
.text:00401687                  call    sub_401030
.text:0040168C                  aeskeygenassist xmm2, xmm3, 20h
.text:00401692                  call    sub_401030
.text:00401697                  aeskeygenassist xmm2, xmm3, 40h
.text:0040169D                  pshufd  xmm2, xmm2, 0FFh
.text:004016A2                  movdqu  xmm4, xmm1
.text:004016A6                  pshufb  xmm4, xmm5
.text:004016AB                  pxor    xmm1, xmm4
.text:004016AF                  pshufb  xmm4, xmm5
.text:004016B4                  pxor    xmm1, xmm4
.text:004016B8                  pshufb  xmm4, xmm5
.text:004016BD                  pxor    xmm1, xmm4
.text:004016C1                  pxor    xmm1, xmm2
.text:004016C5                  movdqu  xmmword ptr [edx], xmm1
```

使用aesenc和aesenclast指令完成加密操作：

```
.text:00404257                  aesenc  xmm2, xmm4
.text:0040425C                  aesenc  xmm3, xmm4
.text:00404261                  movdqa  xmm4, xmmword ptr [ecx+70h]
.text:00404266                  aesenc  xmm0, xmm4
.text:0040426B                  aesenc  xmm1, xmm4
.text:00404270                  aesenc  xmm2, xmm4
.text:00404275                  aesenc  xmm3, xmm4
.text:0040427A                  movdqa  xmm4, xmmword ptr [ecx+80h]
.text:00404282                  aesenc  xmm0, xmm4
.text:00404287                  aesenc  xmm1, xmm4
.text:0040428C                  aesenc  xmm2, xmm4
.text:00404291                  aesenc  xmm3, xmm4
.text:00404296                  movdqa  xmm4, xmmword ptr [ecx+90h]
.text:0040429E                  aesenc  xmm0, xmm4
.text:004042A3                  aesenc  xmm1, xmm4
.text:004042A8                  aesenc  xmm2, xmm4
.text:004042AD                  aesenc  xmm3, xmm4
.text:004042B2                  movdqa  xmm4, xmmword ptr [ecx+0A0h]
.text:004042BA                  aesenc  xmm0, xmm4
.text:004042BF                  aesenc  xmm1, xmm4
.text:004042C4                  aesenc  xmm2, xmm4
.text:004042C9                  aesenc  xmm3, xmm4
.text:004042CE                  movdqa  xmm4, xmmword ptr [ecx+0B0h]
.text:004042D6                  aesenc  xmm0, xmm4
.text:004042DB                  aesenc  xmm1, xmm4
.text:004042E0                  aesenc  xmm2, xmm4
.text:004042E5                  aesenc  xmm3, xmm4
.text:004042EA                  movdqa  xmm4, xmmword ptr [ecx+0C0h]
.text:004042F2                  aesenc  xmm0, xmm4
.text:004042F7                  aesenc  xmm1, xmm4
.text:004042FC                  aesenc  xmm2, xmm4
.text:00404301                  aesenc  xmm3, xmm4
.text:00404306                  movdqa  xmm4, xmmword ptr [ecx+0D0h]
.text:0040430E                  aesenc  xmm0, xmm4
.text:00404313                  aesenc  xmm1, xmm4
.text:00404318                  aesenc  xmm2, xmm4
.text:0040431D                  aesenc  xmm3, xmm4
.text:00404322                  movdqa  xmm4, xmmword ptr [ecx+0E0h]
.text:0040432A                  aesenclast xmm0, xmm4
.text:0040432F                  aesenclast xmm1, xmm4
.text:00404334                  aesenclast xmm2, xmm4
.text:00404339                  aesenclast xmm3, xmm4
```

声 明

NSFOCUS

产品动态

绿盟科技产品更新提示

1.1 网络入侵防御/检测系统规则库更新

网络入侵防御 / 检测规则库最新版本	规则更新
5.6.10.16172	新增规则： 1. 攻击 [24060]:Microsoft Edge 远程内存破坏漏洞 (CVE-2017-8496) 2. 攻击 [24061]:Microsoft Edge 远程内存破坏漏洞 (CVE-2017-8497) 3. 攻击 [24059]:Microsoft Windows LNK 远程代码执行漏洞 (CVE-2017-8464) 4. 攻击 [41498]: 暗云木马通信 5. 攻击 [41498]: 暗云Ⅲ木马通信 6. 攻击 [24007]:Windows 远程桌面代码执行漏洞 (Shadow Broker ESTEEMAUDIT) 7. 攻击 [24006]:Adobe Acrobat Reader 堆缓冲区溢出漏洞 (CVE-2017-2959)
	修改更新规则： 1. 攻击 [23994]:Windows SMB 远程代码执行漏洞 (Shadow Brokers EternalBlue) 攻击 [23808]: HTTP 协议 URI 字段超长 2. 攻击 [24005]:Samba 远程代码执行漏洞 (CVE-2017-7494)

1.2 绿盟科技荣获亚洲信息管理网络奖

近日，NetworkWorld Asia（NWA）颁发的2017年信息管理奖项评选中，绿盟威胁和漏洞管理方案荣获“最有前途的威胁管理解决方案”称号。

绿盟科技已连续两年荣获NetworkWorld Asia的奖项，该奖项表明绿盟科技作为行业领先的网络安全提供商和值得信赖的合作伙伴的市场地位，能够帮助企业提供跨多种威胁的强大的集成网络安全保护。

解决方案概述

绿盟威胁和漏洞管理方案（NSFOCUS Threat and Vulnerability Management Solution，简称NSFOCUS TVM）提供漏洞管理的全过程支撑，量化跟踪和分析流程执行情况，促进管理流程持续优化。同时充分利用绿盟科技威胁情报中心（NTI）的漏洞情报信息，由情报触发流程运转，帮助客户建立快速响应机制，及时有效完成漏洞修补工作。

✓ 情报驱动快速修复漏洞

绿盟威胁和漏洞管理方案通过绿盟威胁情报中心获取漏洞披露情报，结合本地资产信息精确分析漏洞对业务的影响，对可能存在漏洞的资产精确预警。运维人员能够快速进入漏洞管理流程，及时发现漏洞并修补。

✓ 多维度漏洞优先级建议

绿盟威胁和漏洞管理方案引入漏洞攻防情报，如漏洞炒作热度、漏洞利用活跃度信息，结合本地业务资产重要程度，综合多种维度分析关键漏洞风险，给出漏洞处置的优先级建议。

✓ 漏洞全过程管理

绿盟威胁和漏洞管理方案从漏洞披露开始，持续监控资产变化，实时获取漏洞披露情报，对漏洞发现、分析、修补和审核过程进行跟踪，通过对整

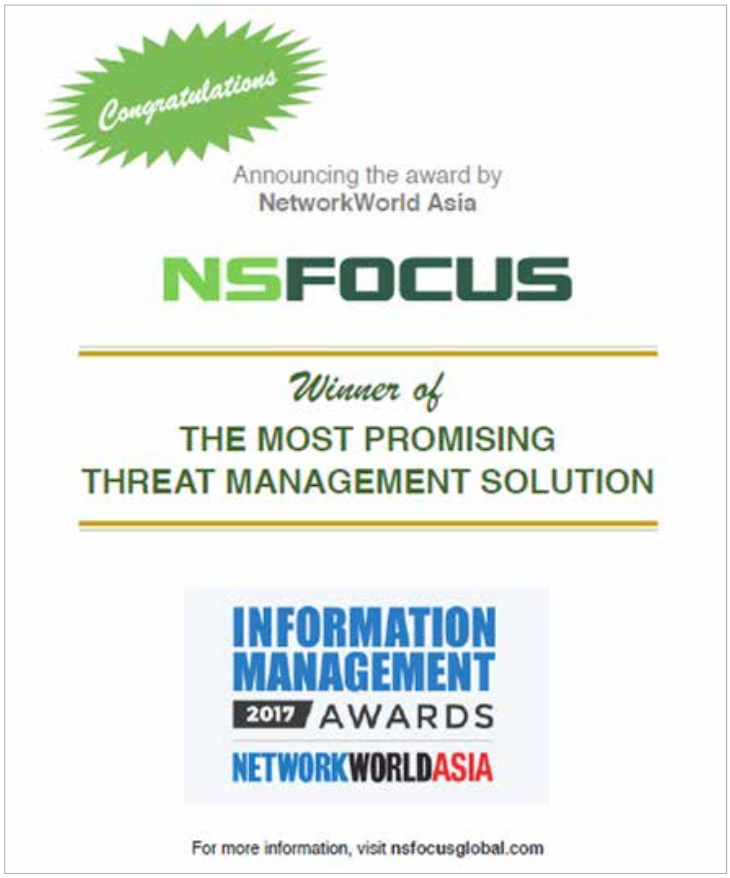
个管理过程的评估、对比，达到持续优化漏洞管理基准要求的目的。

✓ 内外网资产持续监控

利用绿盟威胁情报系统的云端大数据采集能力，能够快速大规模发现企业暴露在互联网上的资产和安全状况。利用本地资产采集设备，全面采集内网资产信息。绿盟威胁和漏洞管理方案持续跟踪网络资产变更，及时发现非合规资产新入网、端口服务变化等问题带来的风险。

NetworkWorld Asia信息管理奖

NetworkWorld Asia信息管理奖创立于2012年，过去几年中该奖项致力于表彰亚洲信息安全、存储与数据管理等领域的行业领导者取得的巨大进步。同时，它也是亚洲这一成熟并不断增长的细分市场内唯一的区域性编辑选择奖，并且得到了Network World Asia、Networks Asia、Security Asia与Storage Asia等亚洲领先出版物及门户网站的鼎力支持。该奖项评委组由拥有丰富知识储备的业内资深编辑指导团队与信息管理领域拥有深刻行业洞察的首席信息官评审团队组成。



防火墙产品使用小技巧
日志分析助力完成策略配置检查及排错

防火墙作为企业网络边界的关键设备，在提供高级访问控制等安全防护功能的同时，往往还承担着路由转发、NAT等基础的网络功能，防火墙运行可靠性要求非常高；

但由于业务变更需要，防火墙策略的变更相对比较频繁，在策略调整后如何有效验证策略配置的正确性和有效性至关重要，而光靠网络或业务测试并不能准确定位是哪一条策略被执行。

假设如下场景：

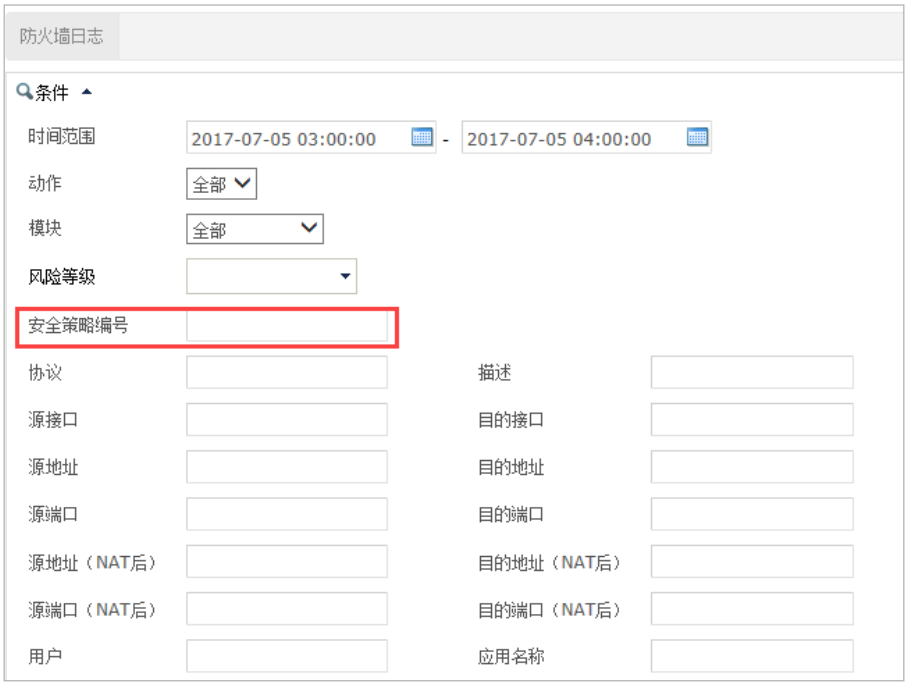
ACL1：允许172.16.10.0/25网段访问内网ip段；

ACL2：允许172.16.10.250主机访问内网ip段；

而假设策略配置时发生错误，错误的将172.16.10.0/25填写为172.16.10.0/24。

这样在业务测试的时候测试业务正常，同时日志显示放行而忽视了策略实质配置错误，带来业务风险。

绿盟科技下一代防火墙日志查询功能支持安全策略查询，用户只需在日志查询时输入安全策略编号，即可对每一条安全策略匹配的日志进行筛选，在网络及业务测试后可使用安全策略编号进行日志筛选，确保策略配置正确，同时也为策略排错提供帮助。



绿盟邮件高级威胁解决方案

轻松应对APT攻击、勒索病毒攻击等高级邮件威胁

邮件高级威胁净化器

全面 | 精确 | 及时

适配通用邮件网关，
隔离APT攻击邮件，
未知勒索软件等高级威胁

THE EXPERT
BEHIND GIANTS
巨人背后的专家

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

NSFOCUS绿盟科技

安全月刊

绿盟科技金融事业部

主 办：绿盟科技金融事业部
地 址：北京市海淀区北洼路 4 号益泰大厦 3 层
邮 编：100089
电 话：010-59610688-1159
传 真：010-59610689
网 站：www.nsfocus.com
客户支持热线：400-818-6868
股票代码：300369

欢迎您扫描目录页左下角二维码，关注绿盟科技、绿盟科技金融事业部官方微信。

月刊电子版下载：http://www.nsfocus.com.cn/research/list_145_145.html