安全月刊

01
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

NSFOCUS

年度盘点

2016年金融行业的信息科技继续蓬勃发展，技术创新层出不穷。

2016年金融行业发生了哪些“大事件”，绿盟科技金融事业部为您盘点.....

本期看点 HEADLINES

P 7 《商业银行信息科技风险管理指引》解读[上]

P 13 年度盘点：2016年金融安全大事记

目录 CONTENTS

政策解读

P07 《商业银行信息科技风险管理指引》解读[上]

年度盘点

P13 年度盘点：2016金融安全大事记

行业研究

P27 金融行业数据安全建设思路分析

P31 期货信息系统安全架构设计

P40 浅析DDOS攻防

P46 Odinaff木马是土耳其金融攻击幕后黑手

P47 攻击乌克兰电网的黑客组织变身TeleBots攻击乌克兰银行

P49 Odinaff木马是土耳其金融攻击幕后黑手

P52 新型针对ATM的恶意软件出现

P54 银行大劫案再袭：多国银行被盗损失惨重

P56 银行木马Dyre新变种悄然来袭亚太

漏洞聚焦

P61 Apache HTTPD拒绝服务漏洞安全威胁通告

P64 Firefox跨域设置cookie漏洞安全威胁通告

P69 Roundcube命令执行漏洞安全威胁通告

P72 ImageMagick压缩TIFF图片远程代码执行漏洞安全威胁通告

P73 OpenSSH远程代码执行漏洞 安全威胁通告

产品动态

P77 绿盟WEB应用防火墙系统（WAF）V6.0.6.0正式发布

P79 DDOS攻击混合清洗方案

P80 堡垒机SAS-H产品使用小技巧

绿盟科技官方微信

绿盟科技金融事业部

绿盟云
NSFOCUS CLOUD

网站安全防护(主机版)

网页防篡改、轻松结合DevOps、网站性能零影响

多重篡改防护

- 采用第三代防篡改技术（增强型事件触发+内核文件底层驱动过滤技术）防护对网站起多层次防护
- 一体化的安全防护和监测，保证网站正常运行
- 支持多网站，多服务器防护
- 支持断线状态下阻止篡改
- 支持连续性篡改防护
- 可靠的实时网页篡改检测

稳定、可靠的客户端

- 可靠的客户端程序，对服务器资源零影响
- 自身进程安全防护，防止非法停止
- 防止自身程序文件、配置文件、日志文件非法修改和删除

快速集成，不影响现有运维习惯

- 开放运维API，可以快速集成到运维脚本中
- 网站运维流程不发生变化，大大提高工作效率

SaaS模式，使用便捷

- 一键安装，安装程序自动适配系统环境
- 云端控制，统一管理，随时随地了解安全变化

NSFOCUS

二 政策解读

NSFOCUS

政策解读 II

《商业银行信息科技风险管理指引》解读【上】

□ 文/绿盟科技金融事业部 高级安全顾问 王宁

一、概述

信息科技风险监管是银监会将在长期进行的重要工作，开始于2006年。通过几年的工作积累，此项工作已经逐步展开并影响到全国的各个银行及相关机构。

银监会在2006年发布《银行业金融机构信息系统风险管理指引》，标志着全行业IT相关的风险管理工作正式开展，同期发布的《关于开展2006年度信息科技风险内部和外部评价审计的通知》（313号文）及其附件，是银行进行具体审计工作的指导性文件。

全国相关的银行机构据此进行了IT系统风险的内审与外审工作，并将结果上报到银监会。2009年3月，银监会发布了新一版的指引，并将其名称变更为《商业银行信息科技风险管理指引》，银行业信息科技风险管理工作进入了新的阶段。

2015年底，伴随着国家十三五规划的发布，银监会政策研究局副局长廖媛媛在银监会召开的有关盘点银行业“十二五”展望“十三五”的新闻发布会上表示：结合中央的“十三五”规划建议的五大理念和银监会党委的要求，“十三五”期间，银行业的发展应当更加注重六大方面。其中一方面就强调要注重金融安全，而金融安全的核心关注点就是风险管理。

> *第五要更加注重金融的安全。首先要持续提升银行业金融机构对信用市场、流动性操作风险等方面的识别应对能力，加强全面风险管理能力，加强信息科技安全系统建设，充分发挥监管者的主动性和前瞻性，坚持风险为本的监管原则，进一步强化风险监管，保护存款人和其他客户的合法权益，不断提升银行业系统性风险监管有效性，维护银行业安全稳健运行，坚决守住不发生系统性、区域性风险的底线。*

经过几年的建设，目前部分银行已经开展了信息科技相关的风险管理工作， 但仍有大多数银行尚未开始或尚未完成信息科技风险管理工作。依照国家有关法律、等级保护要求，银监会有关规定以及ISO27001国际标准的要求，商业银行应通过信息科技风险评估，实现对商业银行信息科技风险的识别、计量、评价和控制；建立信息科技风险管理的三道防线，并通过体系的有效实施、运作、维护和完善，使风险降低到可以接受的程度，同时提升银行的信息安全管理水平和市场竞争力。

在这种形势下，商业银行为了贯彻落实《指引》的各项规定与要求，强化信息科技风险管理工作，提高自身信息安全管理能力，需要制订相应的明确工作方案。绿盟科技金融事业部从建设和咨询的角度出发对《商业银行信息科技风险管理指引》进行解读，为银行在信息科技风险管理工作中提供参考借鉴。

二、《指引》内容解读

银监会相关负责人在答记者问时指出：“和原《指引》相比，新《指引》具有以下六个较鲜明的特点：

一是管理范畴由信息系统风险拓展至信息科技风险，全面覆盖了商业银行信息科技活动的各个环节，进一步明确了信息科技与银行业务的关系；

二是适用范围由银行业金融机构变为法人商业银行，其他银行业金融机构参照执行；

三是信息科技治理作为首要内容提出，充实并细化了对商业银行在治理层面的具体要求；

四是以三个独立章节的内容阐述了信息科技风险管理和内外部审计要求，特别是要求审计贯穿信息科技活动的整个过程之中；

五是参照国际国内的标准和成功实践，对商业银行信息科技整个生命周期内的信息安全、业务连续性管理和外包等方面提出高标准、高要求，使操作性更强；

六是加强了对客户信息保护的要求。”

本次颁布的新《指引》共十一章七十六条，将对我国银行业信息科技风险管理产生积极作用。首先，《指引》规定了董事会和高级管理层在信息科技风险管理中承担的主要责任，提出要构建信息科技风险管理的“三道防线”（即信息科技管理、信息科技风险管理、信息科技风险审计），要求商业银行在决策层设立首席信息官，有利于商业银行加强信息科技治理；其次，新《指引》对商业银行在具体操作层面提供了可供借鉴、操作性强的较高要求，有利于促进商业银行信息科技风险管理水平的持续提升；另外，对敏感信息保护要求的提出，特别是对外包服务环节信息保护的要求，将促使商业银行进一步加强客户信息保护，为广大储户提供更加安全的服务。

第一章 总则

明确了指引的目标和适用范围，指出信息科技是指计算机、通信、微电子和软件工程等现代信息技术，在商业银行业务交易处理、经营管理和内部控制等方面的应用，并包括进行信息科技治理，建立完整的管理组织架构，制订完善的管理制度和流程。信息科技风险管理的目标是通过建立有效的机制，实现对商业银行信息科技风险的识别、计量、监测和控制，促进商业银行安全、持续、稳健运行，推动业务创新，提高信息技术使用水平，增强核心竞争力和可持续发展能力。

第二章 信息科技治理

提出了信息科技治理的要求，明确了信息科技风险管理的责任人，董事会的相关职责，并明确要求商业银行应设立或指派一个特定部门负责信息科技风险管理工作，并直接向首席信息官或首席风险官（风险管理委员会）报告工作。

银监会在监管工作中清楚认识到：银行领导在信息科技风险管理方面，普遍没有给予足够的重视。因此银监会明确了董事会和高级管理层在其中的责任，为信息科技风险管理建立必要的信息科技治理环境，打下必要的基础。信息科技风险管理工作涉及到全行三个重要条线，并需要各行人员的配合与执行，因此董事会和高级管理层应起到实际的领导与指导作用，协调各条线之间的关系，信息科技风险管理才能真正抓好与落实。

首席信息官的职责设定，还可以参考银监会内部征求意见的《商业银行首席信息官办法》。虽然未正式发布，但也有一定的参考价值。

本章确立了“三道防线”，明确了商业银行风险管理部门、信息科技部门以及内部审计部门在信息科技风险管理中承担不同的角色和职责，互相协作共同完善信息科技风险管理的架构。

本章还提出“商业银行应设立或指派一个特定部门负责信息科技风险管理工作”，此部门从长期看，在该银行已经基本实现“全面风险管理”或向这个方面靠拢的情况下，应该是银行的风险管理部门；如果银行的风险管理工作仍然分散在各个条线，如风险管理部门主要管理信用风险，运营管理部管理操作风险等，那么信息科技风险管理工作可能首先需要由IT部门承担，但这不能完全符合银监会的“三道防线”要求。这类银行可能需要配合整体风险管理理念的步调，来最终确定究竟是哪个部门牵头负责。

第三章 信息科技风险管理

要求商业银行应制定符合银行总体业务规划的信息科技战略、信息科技运行计划和信息科技风险评估计划，制定全面的信息科技风险管理策略，建立持续的信息科技风险计量和监测机制。本章是从信息科技风险管理部门的角度，提出商业银行信息科技风险管理的事前控制。

绿盟科技在服务实践中发现，国内大部分银行都缺少明确的长期发展目标，IT部门也同样缺少信息科技战略与相应规划。银监会要求信息科技战略、运行计划等依据总体业务规划来实现，是十分必要的，这样才能保证信息科技风险管理工作能真正支撑银行业务和整体发展。

本章的主要内容还要求银行建立信息科技风险管理策略，这是整体工作的重要组成部分。信息科技风险管理策略内容与第四章的信息安全内容看似有所重复，其实它是信息科技风险管理部门的工作框架，风险管理策略与相关的文档即为其工作内容。

本章工作中，信息科技风险的计量与监测机制是难点，绿盟科技在项目实践中研究总结出了一套有较强落地性的方法，选取风险的各方面关键点与指标形成监测体系，并结合银行现有技术平台进行收集、分析与评价，并实时提示重要信息与告警，达到了阶段性的目标。（未完待续）

NSFOCUS

年度盘点

NSFOCUS

年度盘点

年度盘点：2016年金融安全大事记

文/绿盟科技金融事业部 高级安全顾问 张龙飞

引言

2016年金融行业的信息科技继续蓬勃发展，技术创新层出不穷，大数据、云计算、区块链和移动互联等方方面面的技术摸索和尝试都在为提升公众服务体验做出贡献，而信息泄露、钓鱼诈骗、网络入侵、业务中断等安全事件的发生却一次次的给我们敲响了警钟。中国人民银行（以下简称“人行”）、中国银行业监督管理委员会（以下简称“银监会”）、中国保险监督管理委员会（以下简称“保监会”）、中共中央网络安全和信息化领导小组办公室（以下简称“网信办”）、中华人民共和国公安部（以下简称“公安部”）、中华人民共和国工业和信息化部（以下简称“工信部”）等多个监管机构在这一年对金融行业也开展了全面的网络安全检查工作。这一方面表明保障金融行业信息安全的重要性，另一方面也表明金融行业对自身信息安全需要提出更高的要求。

> “千丈之堤，以蝼蚁之穴溃；百尺之室，以突隙之炽焚。”
>
> ---《韩非子》

伴随着国家互联网信息办公室《国家网络空间安全战略》的颁布，2016年也已与我们渐行渐远，回顾这一年发生的点点滴滴，算不上惊心动魄,却也是跌宕起伏。前车之鉴,后事之师，知攻才能善守，知漏才能补缺。本文通过分析整理2016年金融行业安全事件和热点事件，从以下8个方面来总结金融行业面临的行业现状、监管要求、安全风险等，也给金融行业的2017年信息安全建设给出可落地的参考建议。

监管文件抢头条　移动终端是热点

信息泄露成常态　钓鱼欺诈手段多

内网问题隐藏深　里应外合要警惕

外网防线待加强　应急机制需落地

1 监管文件抢头条

关键词：107号文 261号文 网络安全法 国家网络空间安全战略

概述：2014年被称为是中国网络安全元年，2015年是互联网金融野蛮生长的一年，而2016年可以被称为金融安全监管的一年，这一年不论从行业监管层面，还是从国家监管层面都密集的发布了相关的要求文件，中国人民银行、银监会、保监会、网信办、公安部、工信部等部门每月都有相关的文件要求或安全通告下发，而金融机构进行网络安全自查和配合网络安全检查或联合执法检查也贯穿了全年。监管文件在这一年也成功抢占了各大新闻媒体、公众号自媒体的头条位置。

事件回顾：

① 银监办发[2016]107号《中国银监会办公厅关于开展银行业网络安全风险专项评估治理及配合做好关键信息基础设施网络安全检查工作的通知》

② 人民银行《关于加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》银发〔2016〕261号

③ 中共中央办公厅 国务院办公厅发布《国家信息化发展战略纲要》

④ 全国人民代表大会常务委员会《中华人民共和国网络安全法》

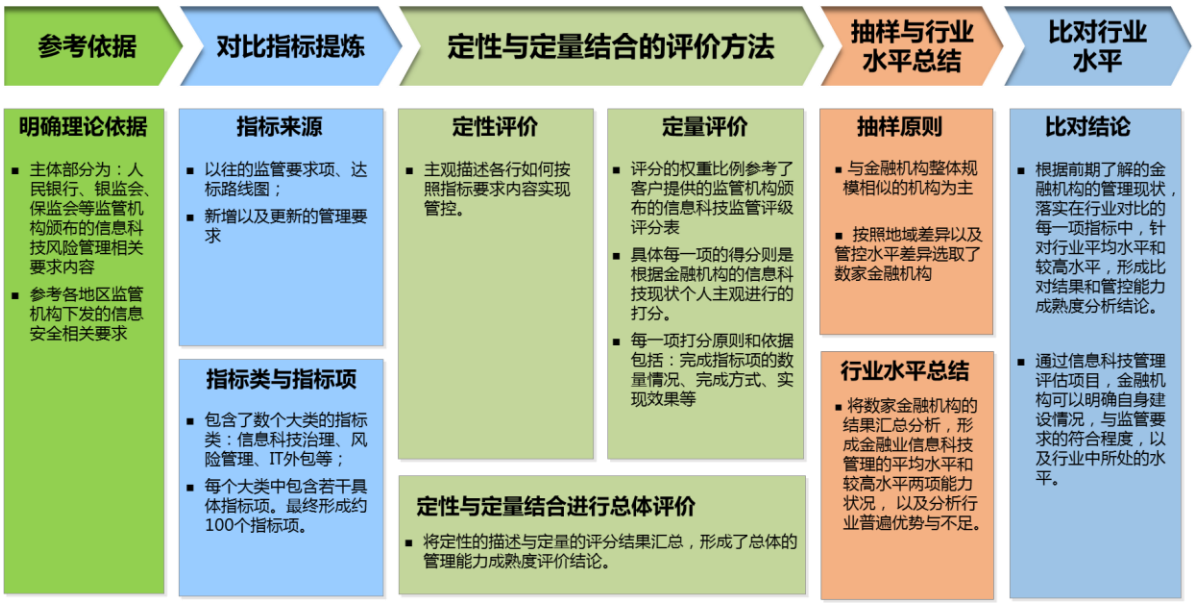
⑤ 国家互联网信息办公室发布《国家网络空间安全战略》

监管要求：

近年，随着网络安全形势的日趋严峻，网络安全也逐步上升到国家层面，《中华人民共和国网络安全法》《国家网络空间安全战略》 的接连发布，多部门联合网络安全专项整治大检查，这一切都表明我国网络安全从法制化到监管落地的实质性展开，金融机构作为关键信息基础设施的运营者，需认清自身的战略地位和价值，提升对网络安全工作的重视程度，在加强对信息安全的投入，有效推动行业信息安全建设，促进行业整体安全防护水平的提升，进一步推进习近平主席提出的“推进网络强国建设，让互联网更好造福国家和人民”。

解决建议：

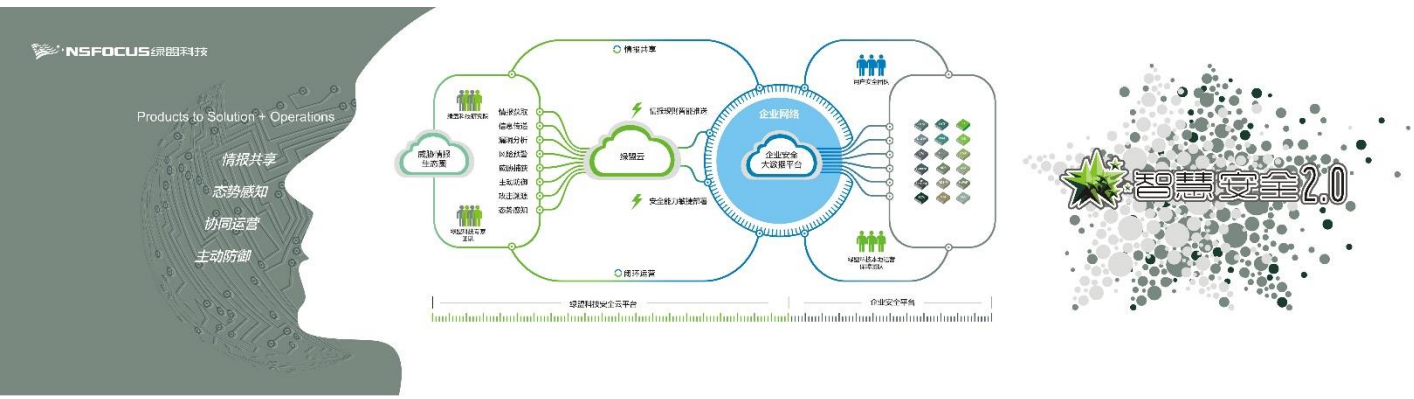
绿盟科技作为绿盟科技作为安全领域的领军企业，深耕专注于专业领域，目前已与超过千余家金融机构建立商业合作，按照国家政策、监管部门及行业相关要求与标准，对信息科技管理现状进行评估，发现信息科技工作有待完善之处，提出改进策略、方案等，构建符合监管要求的信息科技体系，形成制度健全、管理规范、措施有力的信息科技管理体系。



详情请关注绿盟科技金融事业部信息安全月刊或公众号nsfocusfbd文章：

《依据网络安全法构筑金融行业防护体系》

《金融行业等保标准相关要求解读》



2 移动终端是热点

关键词：交易劫持 高危漏洞 伪装篡改 勒索病毒

概述：近年来，移动支付发展迅猛，手机银行作为各大银行推出的电子银行系统，一方面，极大地方便了客户业务办理，提升了消费体验；另一方面，由于前期发展过快，只重视业务覆盖，而对业务安全并没有足够的投入，导致安全问题频出。

事件回顾：

① XPwn2016安全专家：多数手机银行APP可被劫持

② 88个金融类APP被曝10大隐患 安全漏洞亟待打补丁

② 黑客伪装手机银行应用实施攻击

③ 盗号木马伪装手机银行APP图标

④ 澳大利亚多银行手机APP遭黑客攻击

⑤ 勒索病毒盯上移动终端 不交钱就变砖

监管要求：

随着移动终端逐渐已成为银行业业务推广重点的情况，为了应对日趋严重的移动终端安全风险，金融机构在移动终端支付系统的建设中参考了《电子银行安全评估指引》、《银行业金融机构安全评估办法》、《网上银行系统信息安全通用规范》等行业标准，并借鉴了相关国家标准、国际标准的安全要求，并在上线前完成业务的安全评估和应用加固工作。当然也有监管机构发布了针对性的指导文件， 深圳市市场监督管理局于2016年11月4日发布了《金融服务移动应用信息安全指南》，并自2016年12月1日起实施，该文件落地实施对加强金融服务移动应用安全水平具有积极意义。

解决建议：

绿盟科技基于多年的针对金融行业移动应用安全的体系建设的服务经验，结合满足监管合规要求和业务发展的全生命周期两方面进行综合考虑，推出了绿盟科技手机银行App交易安全防护解决方案。

详情请关注绿盟科技金融事业部信息安全月刊或公众号nsfocusfbd文章：《【关注】绿盟科技受邀在<焦点访谈>上说的安全那些事》

3 信息泄露成常态

关键词：账号密码 银行卡 系统漏洞 数据记录 征信报告

概述：信息泄露在这几年的网络发展中是挥不去的阴影，在2016年，几乎每天都会看到信息泄露的新闻，从平凡百姓信息泄露导致经济损失到美国“邮件门”影响总统选举，足见信息泄露造成的影响是不堪设想的。而金融机构拥有用户个人真实信息及经济信息，这些信息一旦被泄露、盗取甚至售卖，不仅严重威胁了用户的资金安全，也为电信诈骗创造了条件。

事件回顾：

① 某保险公司数百万保单记录和支付信息被爆有泄露风险

② 员工倒卖征信报告200余万条涉案资金100余万元

③ 网曝京东电商12G的数据包在网络上流传

④ 网易过亿邮箱数据疑似泄露

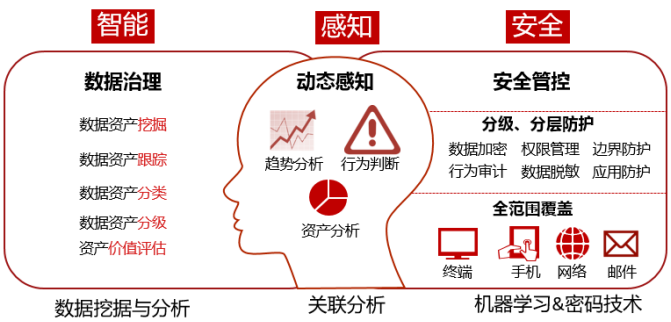
⑤ 百度网盘遭遇撞库,50万账号被盗

监管要求：

2016年人民银行印发《中国人民银行金融消费者权益保护实施办法》，明确了金融机构在保护个人信息方面的责任和义务，不得非法使用个人信息，并采取有效措施保护个人金融信息安全。《网络安全法》中也明确了金融机构需建立、健全对数据进行分类分级，明确不同类型数据的保护级别，对个人信息和重要业务数据通过备份、加密等方式进行保护，防止个人信息和重要业务数据未经授权访问、篡改和泄密。

解决建议：

按照金融行业的安全体系要求，绿盟科技全资子公司亿赛通推出的Next Generation DLP 下一代数据泄露防护系统，完全可以满足行业需求。该系统是指融合机器学习、大数据、关联分析、密码、访问控制、数据标识技术，对结构化和非结构化数据进行数据治理、安全管控、态势感知，以达到数据泄露防护效果的解决方案。



详情请关注绿盟科技金融事业部信息安全月刊或公众号nsfocusfbd：《【创新方案】三步走加强金融行业敏感数据泄露防护》

4 钓鱼欺诈手段多

关键词：电话 邮件 短信 链接 U盘 文件 伪基站 二维码

概述：2016年发生的“山东徐玉玉案”几乎家喻户晓，也打响了我国打击电信诈骗的号角，公安部门统计，2013年以来，全国共发生被骗千万元以上的电信诈骗案件104起，百万元以上的案件2392起。而金融机构作为打击电信诈骗的重要一环，应承担不可推卸的社会责任和义务。

事件回顾：

① “徐玉玉案”揭秘“诈骗黑色产业链”

② 诈骗团伙发木马短信男子点链接11万不翼而飞

③ 诈骗团伙利用“伪基站”诈骗致使60万手机通讯中断

④ 偷换二维码盗刷百万 以商业广场内的小食店奶茶店为目标

⑤ 澳洲警方警告居民小心信箱当中的不明U盘藏木马

监管要求：

2016年国家网络安全宣传周 “金融日”期间，金融行业围绕“普及知识•防范诈骗•增强信任”为宣传重点，开展防范金融网络诈骗主题宣传。银监会印发《关于银行业打击治理电信网络新型违法犯罪有关工作事项的通知》，中国人民银行发布《关于加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》，中国银监会、公安部正式对外发布《电信网络新型违法犯罪案件冻结资金返还若干规定》，对银行业打击治理电信网络新型违法犯罪工作进行了全面部署。

解决建议：

为了应对打击电信诈骗等监管要求，绿盟科技推出安全咨询与培训服务，从多个不同维度考虑来设计培训课程以满足企业客户获取安全知识和经验的需求，从而使客户最终达到理解监管要求，强化安全意识，掌握安全技术，获得安全实践经验，能够融会贯通并应用于所在企业的安全建设当中。

预警体系		控制体系					响应体系		
现场交互类		日常提示类					物品提示类		
意识培训	各种交互活动	动态banner	张贴标语	警示便签	屏幕保护	易拉宝	小物品	分发小册子	电子杂志
线上的培训材料；线下讲座类	模拟场景/在线问答等	在网站或各种服务的登录页面放置安全提示	在营业厅显眼处放置张贴画	在电脑、门禁等处张贴安全提醒便签	提供安全意识培养屏保	安全宣传活动中展现企业安全警讯、口号等	包含安全提示的各种定制小物件	印刷制作安全手册，分发客户教育手册	专题形式的教育电子杂志

详情请关注绿盟科技金融事业部信息安全月刊或公众号nsfocusfbd文章：

《【观点】防金融欺诈国内银行应可做的更多和更好》

《盘点 | 2016电信诈骗屡屡得手，金融数据如何系好“安全带”？》

5 内网问题隐藏深

关键词：SWIFT ATM POS 勒索病毒 0day APT

概述：近些年发现的黑客组织攻击活动趋利性明显，金融机构作为与金钱直接相关的机构成为了攻击的主要目标。2016年出现了多起银行大劫案，通过对这些事件进行综合分析发现，黑客组织往往会使用新型的攻击手段，绕过传统安全机制的检测和防御，长期的潜伏进银行内部业务系统发起攻击，如SWIFT系统、ATM机等。这些事件给金融机构造成了严重的经济损失和信任危机。

事件回顾：

① 孟加拉国央行被黑客攻击导致8100万美元被窃取

② SWIFT警告全球银行或遭新一轮网络攻击

③ 多家银行内部人员遭到勒索邮件攻击

④ 多家知名酒店集团POS系统感染恶意软件

⑤ 亚欧14国ATM机被攻击自动吐钱

监管要求：

针对日趋严峻的金融安全威胁形势， 2016年银监办发[2016]107号《中国银监会办公厅关于开展银行业网络安全风险专项评估治理及配合做好关键信息基础设施网络安全检查工作的通知》，文件明确要求开展高级持续性威胁专项评估工作，政策性银行、大型银行、股份制银行、邮储银行还要针对高级持续性威胁、精准式网络攻击进行安全评估，对威胁和攻击进行分类场景设定，有针对性的排查系统漏洞、分析脆弱性；形成应对此类攻击的防护措施专项评估报告。

解决建议：

针对金融行业安全运维应对新型攻击的防御需求，绿盟科技推出下一代威胁防御（NGTP）解决方案可以有效的从网络、邮件和终端层面抵御安全威胁的侵入，可针对包括APT攻击在内的威胁进行检测和防御。方案以检测未知威胁为核心，通过智能网管和大数据分析技术，对来自终端、安全网关、操作系统的告警信息进行综合分析、可视化呈现和管控，极大的提升了企业安全防护能力。

详情请关注绿盟科技金融事业部信息安全月刊或公众号nsfocusfbd文章：

《SWIFT银行结算系统攻击事件分析》

《邮件勒索病毒的分析与防护》

《【案例分享】勒索病毒？绿盟下一代威胁防御方案轻松应对》

6 里应外合要警惕

关键词：征信报告 银行职员 银行行长 倒卖获利 外包风险

概述：2016年震惊全国的“5•26侵犯公民个人信息案”,抓获包括银行管理层在内的犯罪团伙骨干分子15人、查获公民银行个人信息257万条、涉案资金230万元，也将征信产业乱象公之于众，折射出征信监管的严重缺失。

事件回顾：

① 监守自盗 广西来宾一银行员工倒卖9300多人信用报告

② 湖北多名银行职员倒卖储户信息 非法获利近20万

③ 银行员工倒卖征信报告 泄露信息200余万份资金100余万

④ 257万条公民银行个人信息被泄露 银行行长卖账号

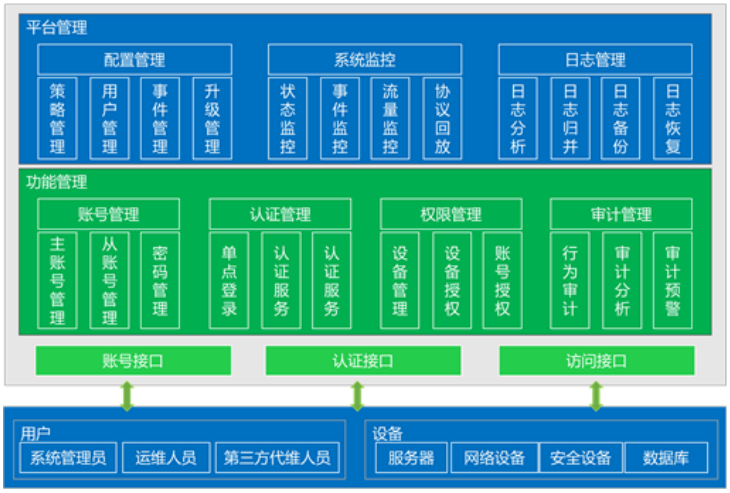
⑤ 外包服务存隐患 银监会提示银行信息泄露风险

监管要求：

人民银行发布《关于加强征信合规管理工作的通知》，银监会下发《关于银行业金融机构客户个人信息泄露案件风险提示的通知》，直指部分银行在内控方面存在严重问题，业务外包管控不力，缺乏有效制约，并且明确要求金融机构要充分认识保护客户个人信息安全工作的重要意义，切实落实主体责任，完善客户个人信息保护制度建设，强化执行管理。

解决建议：

绿盟科技通过对征信系统使用存在的威胁与风险分析，并挖掘金融机构的征信系统信息安全需求，推出商业银行个人征信系统安全托管平台解决方案，实现对征信系统访问的集中精细化操作管控与审计，有效规范征信系统的使用，满足监管部门的合规管理要求。



详情请关注绿盟科技金融事业部信息安全月刊或公众号nsfocusfbd文章：

《商业银行征信系统安全防护解决方案》

《祸起萧墙：从“5.26信息泄露案”谈银行征信系统数据库安全防护》

7 外网防线待加强

关键词：系统漏洞 逻辑漏洞 DDOS 弱口令 开发安全 第三方接入

概述：近年来，随着互联网的迅速发展，金融机构为了应对“互联网+”的冲击，纷纷推出各种依托互联网的业务系统来更好的满足用户的需求。据绿盟云网站安全监测数据显示：在监控的12728个网站中发现了611356个安全漏洞，其中高危漏洞24663个，并协助抵御数百万次黑客攻击。面对日益严峻的网络安全形势，金融机构需要加强外网防线以应对安全威胁的考验。

事件回顾：

① 九成银行在线系统有安全漏洞

② 某保险机构信息系统多次被曝存在高危漏洞

③ 某银行第三方接口漏洞导致严重经济损失

④ 银行系统升级出漏洞 两人钻空子套现2000多万

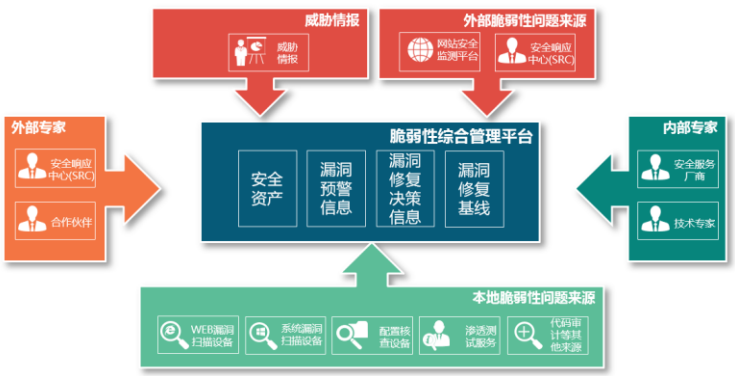
⑤ 银行ETC联名卡盗刷事件折射产品设计漏洞

监管要求：

2016年人民银行、银监会、保监会等监管机构发布风险评估相关工作办法，明确要求进一步加强互联网安全风险应对，提升银行业整体防护能力。《网络安全法》也明确要求金融机构作为关键信息基础设施的运营者，需更进一步明确自身应当履行的责任和义务。在组织架构、安全管理、安全技术等多个方面做好工作落实，如等级保护、风险评估、数据保护、日志留存、应急响应等。

解决建议：

针对现在安全漏洞在互联网传播迅速，被利用时间短，对网络爆发式影响的特点，结合多年的安全研究和服务经验，绿盟科技提出了金融行业脆弱性管理平台，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。同时充分利用漏洞情报信息，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。



详情请关注绿盟科技金融事业部信息安全月刊或公众号nsfocusfbd文章：
《金融机构与第三方平台对接的风险分析及安全防护》
《浅析短信验证码的风险和防范》
《绿盟科技金融行业脆弱性管理平台荣获“2016企业优秀解决方案奖”》

8 应急机制需落地

关键词：供电中断 UPS故障 业务切换 网络中断 暴雨灾害 雷电灾害

概述：应急机制包含应急预案、应急演练和应急响应，是安全运维的重要工作。但是在现实生活中，大多数应急机制都停留在案头文件上，业务上线切换失败、UPS供电故障、数据丢失损坏、黑客网络攻击、勒索邮件传播等安全事件发生导致的银行业务中断还是屡见不鲜。

事件回顾：

① 北京亦庄某数据中心供电中断致数十家银行业务中断

② 匿名者开始行动:攻击至少导致4家银行网站关闭

③ 汇丰网银遭网络攻击 不到一个月瘫痪两次

④ 英国乐购银行数万账户被盗 被迫停止线上交易

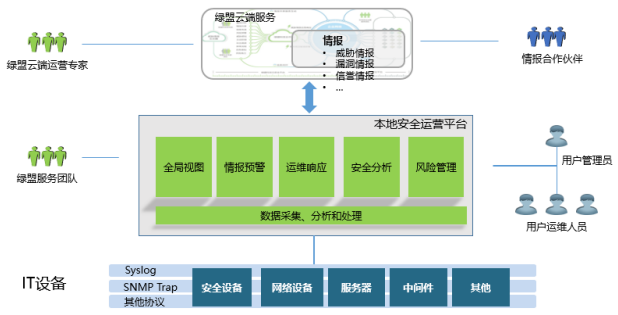
⑤ 回顾韩国农信社“安全门”：数据清空 备份失效

监管要求：

银监办发[2016]107号《中国银监会办公厅关于开展银行业网络安全风险专项评估治理及配合做好关键信息基础设施网络安全检查工作的通知》，文件明确要求开展网络安全应急预案评估和网络安全应急演练工作，对该项工作突出的单位，银监会将工作情况纳入监管评级结果中。《网络安全法》要求金融机构需建立、健全安全事件应急和响应、通报等安全风险全流程闭环管理机制，结合国家层面网络安全监测预警和信息通报制度，统筹加强各类网络安全事件和风险的监测、通报，协同联动国家力量共同处置互联网安全风险。

解决建议：

为了应对金融机构面临的诸多安全运维难题，绿盟科技推出企业安全平台解决方案，以大数据框架为基础，结合威胁情报系统，通过攻防场景模型的大数据分析及可视化展示等手段，协助企业建立和完善安全态势全面监控、安全威胁实时预警、安全事故紧急响应的能力。通过独有的自适应的体系架构，高效地结合情境上下文分析，协助安全专家快速发现和分析安全问题，并能通过运维手段实现全生命周期的安全闭环处理流程。



详情请关注绿盟科技金融事业部信息安全月刊或公众号nsfocusfbd文章：
《众测（Bugs Bounty）的相关分析和安全思考》
《【创新方案】安全大数据分析解决方案》

结　语

他山之石，可以攻玉，2016年发生的安全事件都将成为宝贵的经验财富，为金融机构的信息安全体系建设完善添砖加瓦。金融安全，关乎经济社会发展，关乎千家万户安乐。绿盟科技作为安全领域的领军企业，在新的一年力，将与金融机构精诚合作，助力金融机构轻松应对安全挑战，走上智慧安全运营之路。

NSFOCUS

NGTP V2.0

下一代威胁防御解决方案

Next Generation Threat Protection

网络

邮件

终端

以高级威胁分析为核心，以安全威胁信誉为纽带

关联入侵防御，邮件过滤，终端防护多种防护手段

为企业提供威胁进不来，扩散赢不住，数据带不走的防护效果

2016.01 隆重上市

APT检测和防御解决方案

全面 实时 高效

NSFOCUS

行业研究

NSFOCUS

行业研究

金融行业数据安全建设思路分析

□ 文/绿盟科技金融事业部 高级安全顾问 陈爱珍

前言

随着《网络安全法》的正式颁布，当前我国网络安全方面存在的热点难点问题再一次呈现在众人面前，个人信息泄露事件尤为令人关注，近几年金融行业信息泄露事件呈密集高发趋势，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。

面对安全事件及国家监管压力，金融行业该如何做好数据安全防护工作，防范个人信息泄露风险？针对这个问题，绿盟科技安全专家结合多年的信息安全经验，梳理金融行业数据泄密威胁特点，为金融用户提供一套全方位的数据防泄密建设解决思路。

数据泄密威胁分析

纵观金融行业历年的信息泄露事件，无论是2015年堪称史上最大规模银行泄密的汇丰银行3万账户文件曝光事件，还是2016年“5.26侵犯公民个人信息案”致257万公民银行卡个人信息泄露事件，仔细分析这些触目惊心的案例，究其原因，主要有以下两种类型：

外部黑客入侵：黑客使用非法手段及工具,利用目标系统的漏洞对其进行入侵攻击，例如采取网络监听、SQL注入、口令破解等手段进行非法数据窃取；

内部人员泄露：内部人员在接触数据的处理过程中,人为有意或无意致使数据泄露，例如关键数据岗位人员携带重要用户信息离职、数据库管理员将个人金融信息泄露给竞争对手或其他第三方。

另据美国隐私权利清算所2013年到2015年数据泄密事件报告分析，外部黑客入侵和内部人员泄密已占全部事件的99.99%，且占比一直高居不下，而其他的意外事件泄密、物理记录丢失及设备遗失等原因则少之又少。

数据生命周期及流转途径分析

业界对于数据安全大多按照创建、存储、使用、交换、存档及销毁生命周期来区分管理，但据绿盟科技金融专家认为，全面的数据威胁分析，应在生命周期以上各阶段，结合金融系统重要信息系统业务特点，梳理业务安全逻辑及数据流转路径，评估流转关键节点上的人为和技术脆弱性，有针对性的进行数据防泄密防护。

数据安全建设建议

基于以上分析，我们发现金融行业员工的安全意识欠缺，管理手段的孱弱，技术手段的缺失，导致数据泄漏事件的频频爆发，绿盟科技依靠多年的方案设计经验，将在深入分析金融系统业务安全需求的基础上，为用户提供并建立一套全方位的数据防泄密安全解决方案，方案中不仅包括安全技术体系的部署，而且包括安全组织体系和安全管理体系的建立：

第一步 评估

绿盟科技依据金融行业监管要求及安全威胁，结合各业务系统特点，尤其是重要信息系统，进行数据生命周期及数据流转路径梳理，帮助金融客户构画一套集业务、数据、系统、关键节点及人员岗位的逻辑拓扑图，并形成组织、管理及技术三位一体的全方面数据安全风险清单及评估报告。

第二步 规划：

数据安全风险防范一如信息科技风险建设，绿盟科技不建议客户急于求成、一蹴而就，应依据前期金融用户数据安全风险评估报告及重点风险清单，结合用户行业和业务系统特点、匹配自身安全建设现状，基于此考虑，绿盟科技金融专家团队将为用户提供3-5年的数据安全建设规划，提供一份贴合用户现状且能有效落地实施的数据安全建设规划报告。

第三步 建设：

数据安全体系建设需从组织、管理和技术三方面进行，鉴于篇幅原因，此文我们从以上三方面截取部分进行举例说明：

数据安全组织体系：安全组织体系应重点关注机构建设和人员管理两方面内容：

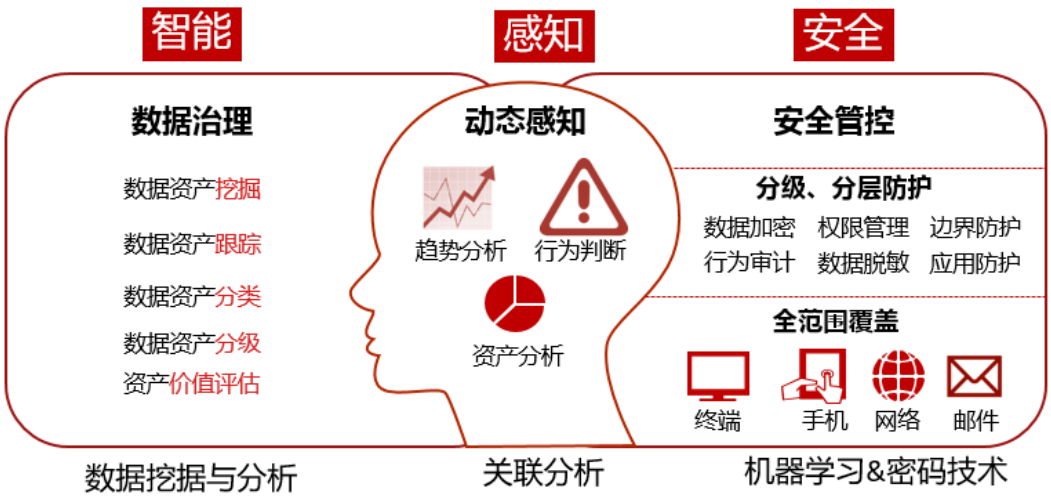
对于数据安全组织体系，绿盟科技认为，最重要的一步就是需要明确数据安全责任部门及岗位：常规的数据安全责任往往落在信息技术部门，但依据金融行业信息科技风险相关管理要求及专家深度分析，与数据密切相连的业务部门及其他数据流转部门也应承担至关重要的数据保密责任，其次，作为二三道防线的风险管理及审计稽核部门也应当明确在数据安全组织体系中的职责划分。

前期事件及威胁分析中，大家已经了解到，人员管理在数据安全组织体系中尤为重要，绿盟科技在评估过程中将梳理形成一份业务系统关键岗位人员构成图，同时响应《网络安全法》及金融行业相关监管要求，应对于重要岗位人员进行入职背景调查，到岗后应定期进行信息科技风险及数据安全意识教育培训，并纳入用户整体考核体系。

数据安全管理体系：数据安全管理作为信息安全体系的一块重要组成部分，绿盟科技建议依据银监会《银行业信息科技风险管理指引》，结合ISO27001最佳实践，将数据安全要求纳入到现有信息科技风险管理体系，规范如核心数据备份及恢复操作安全控制策略及申请流程表单、系统数据变更管理制度、生产数据脱敏使用规范、数据泄密事件应急响应专项预案等一系列数据安全制度要求，建设一套集策略、制度、流程及表单的四级可落地实施数据安全管理体系。

数据安全技术体系：数据安全技术体系作为组织和管理体系的有效支撑工具：

针对外部入侵，需在重要信息系统及核心数据区域进行有效防护，互联网业务一直是金融行业风险高发及重要关注点，应定期进行安全评估及渗透测试，主动发现系统、代码脆弱性并及时加固，必要时应部署专业的WEB安全防护设备进行外部数据泄密监测及拦截。



针对内部人员泄密，系统运维和用户访问一直是金融行业数据泄密的两大高发地，绿盟科技认为运维层面应部署运维安全审计系统，对所有内部及第三方运维管理人员的行为进行监测、防护及审计。重要数据库前端应部署数据库防火墙，对所有用户操作进行主动防护；对于开发、测试、培训环境使用数据必须使用专业的数据脱敏系统进行数据漂白混淆；对于众多且分布广泛的普通数据访问者，则应部署专业的终端数据防泄密系统。㊟

第四步 运行及改进：

当数据安全体系建设上线时，会经历一段落地磨合期，体系是否能按预期顺利运行，取决于上线后的执行情况，绿盟金融专家根据项目实施经验，为每个用户量身打造一套数据安全体系实施推广计划，包括培训、试点运行、意见反馈、改进优化及全面推进等全方位设计，项目团队全程跟进并协助用户逐一消除落地实施障碍，保障数据安全体系确实顺利有效运行，从而确保用户数据安全可控。

（注：受篇幅限制，本文未对方案深入展开阐述，如您对数据安全建设方案感兴趣，请与绿盟科技联系索取更多相关资料并切磋交流。）

期货信息系统安全架构设计

文/绿盟科技金融事业部 高级安全顾问 徐贵敏

云计算、大数据、移动APP等新技术所带来的行业信息技术应用更新和技术场景变化，对信息安全提出了新的挑战。程序化交易、国际化、互联网金融等业务模式创新，要求信息安全适应业务发展的需求，以保障资本市场的健康稳定和可持续发展。同时，需要建立有针对性的期货行业安全保障机制并结合新技术的特点制定相应的风险防范措施，以防范新技术应用衍生风险，保持期货信息系统的安全服务等级和风险应对水平。

一. 引言

互联网技术的迅速发展带来了国际证券期货市场也发生了巨大的变革，传统交易方式纷纷被摒弃，而大力推行网上交易形式，由此，全球性的证券、期货交易网络逐渐形成，对传统的证券、期货公司交易模式带来巨大冲击。但在证券期货网上交易日益普及的今天，一些诸如倒卖盗买按键的发生却屡禁不止，在侵害投资者利益的同时，也将证券期货网上交易的安全性问题摆在了人们的面前。因此，证券期货网上交易的安全性就成为一个迫切需要解决的问题，从安全角度来讨论期货网上交易就显得十分必要，对于证券期货网上交易的长足、稳步开展具有积极的现实意义。

期货行业作为资本市场的一个重要组成部分，对深化经济体制改革、推动企业发展壮大、促进经济结构调整起到了重要的推动作用。期货行业的国内网上交易额占期货交易总额的比例也逐年提升，并呈现出加速发展的趋势，根据最新统计，目前我国期货公司中 90%以上的交易通过互联网进行。 目前我国期货行业的业务开展已高度依赖信息系统。 通过互联网进行网上交易具有成本低、效率高、便捷性和覆盖范围广等优点，因此，网上交易已成为期货交易的主要方式。

网络交易便捷的同时，随之而来安全风险也逐步增加，针对网络黑客的攻击动机和攻击方式的变化带来的网络安全问题，单纯的网络安全防护手段已经难以适应期货网上交易安全要求，为此我们需要通过多个维度建立适应行业发展的安全防护要求。

随着《证券公司信息技术管理规范》、《证券公司集中交易安全管理技术指引》、《证券公司风险处置条例》等一系列行业规定、标准的颁布，监管机构对于证券行业信息安全的理解渐渐由管理和技术保障体系转换到了风险管理层次。

二. 期货行业网络架构方式

当前，期货行业网络架构方式如下：

期货行业网络区域分为：

- 报盘区；
- 银期前置区；
- 广域网接入区；
- 客户托管交易前置区；
- 核心交换区；
- 异地数据中心区；
- 互联网交易区 ；
- 运维管理中心区；
- 系统监控中心区。

三. 期货业务面临的安全隐患

通过对30家证券期货公司信息系统渗透测试结果看：发现85%证券期货企业存在不同程度的安全漏洞，而75%企业存在严重安全漏洞。约50%证券期货企业安全防护能力严重不足，被成功渗入企业内部网络。近25%证券期货企业交易、行情、委托报盘等核心业务能够被完全远程控制，可关闭被控的交易服务器，中断交易服务，影响投资者正常交易；可通过控制的委托报盘系统，伪造大量委托报盘，向交易所发起拒绝服务攻击，进而威胁到证券交易所核心交易系统的安全；可获取用户资金、交易记录、个人信息等核心敏感信息。*（数据来源：证监会委托某检查机构）*

期货行业面临的主要安全隐患包括敏感信息泄露、交易数据篡改以及拒绝服务攻击，具体分析如下：

3.1 敏感信息泄露

2016年3月15日（全称：消费者权益保护人）一组调查，“证券业589项系统漏洞暴露，导致投资者信息泄露”。

“其实IT系统存在BUG是正常的，也是可以被接受的，只是看不同行业，像金融业对系统漏洞的容忍度应该比较低，因为涉及到资金往来，许多信息更加敏感，所以一旦出现外泄后果也更严重。

相应的设计缺陷也曾存在于部分期货公司，例如国内某期货官网主站就被曝存在权限漏洞，而该问题易导致其注册会员的用户名、电话、邮箱、姓名等相关资料出现泄露；此外，该期货公司网站被曝还存在XSS漏洞等问题。

“一些漏洞如果被利用，造成内网信息外泄的后果可能很严重，比如黑客会利用漏洞盗取用户信息，甚至查看到对应的交易动作，进而从事内幕交易。”随着互联网金融的渗透，IT技术在金融业务中的应用更加广泛，证券期货经营机构应进一步提高IT系统的风控及安全建设标准，适应新形势下的网络安全要求。

3.2 交易数据篡改

黑客攻击与服务器入侵获得利益或是盗取名单或是破坏正常交易在交易场所一直都存在。究其原因主要有二点：第一、报复交易场所，如北京石油交易所之前的521事件是投资者在交易场所亏损后进行恶意报复。第二、通过入侵服务器，修改数据获利。国内很多交易场所就出现账目对不齐的情况，这就是被人入侵了服务器，黑客可以轻松从自己设置的一个账户里，通过银行卡取走大量的资金。

造成交易数据被篡改的主要原因，一方面安全防护建设不到位，另一方面缺乏健全的风控管理标注以及应用软件自身的安全性等。

3.3 拒绝服务攻击

鉴于当前安全设备（防火墙、入侵检测等）对DDoS攻击防护能力的不足，当前证券期货业的均采用线上交易，线上交易平台经常是黑客实施DDoS攻击的对象，，该类业务系统遭受DDoS攻击时，系统将无法提供正常服务，而由此引起的业务无法访问、支付错误、交易量下降、品牌损失、系统恢复的代价等等，都会造成直接经济损失。甚至有些黑客还利用DDoS攻击对网站进行敲诈勒索，给线上交易的正常运营带来极大的影响。

四. 期货业建设参考的规范及要求

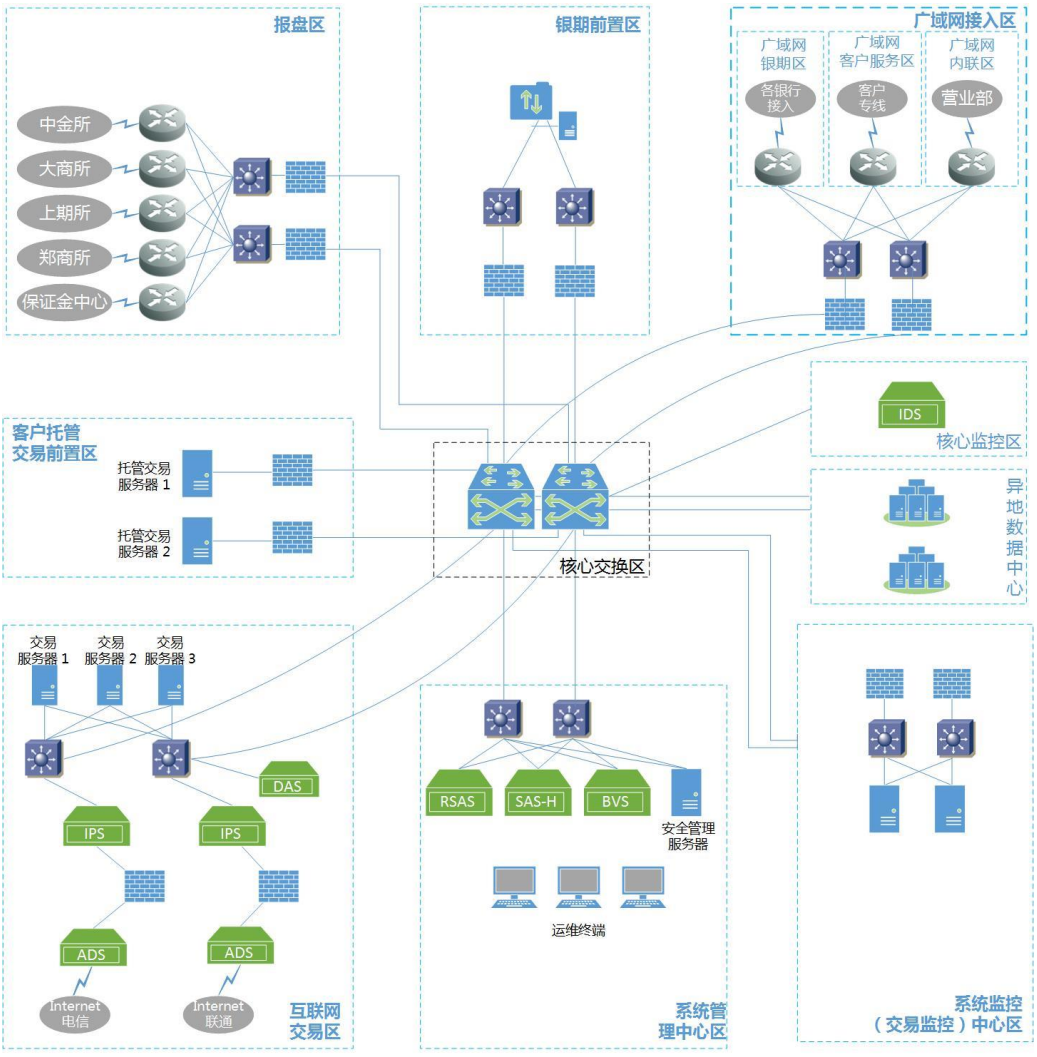
建设参考的规范及要求如下：

- 证券期货业信息安全保障管理办法（证监会令第82号）；
- 证券期货业信息安全事件报告与调查处理办法（证监会公告〔2012〕46号）；
- 关于印发《证券期货市场突发事件应急预案》的通知（证监发〔2012〕97号）；
- 关于印发《证券公司实施<证券期货经营机构信息系统备份能力标准>指导意见》的通知（机构部部函〔2011〕504号）；
- 关于做好证券公司网上交易强身份认证有关工作的通知（机构部部函〔2011〕450号）；
- 关于进一步加强期货公司信息技术管理工作的指导意见（证监会公告〔2009〕15号）；
- 关于加强期货公司信息系统备份能力建设工作的通知（期货二部函〔2011〕597号）；
- 证券公司集中交易安全管理技术指引（中证协发〔2006〕81号）；
- 证券公司网上证券信息系统技术指引（中证协发〔2009〕66号）；
- 期货公司信息技术管理指引（中期协字〔2014〕75号）；
- 期货公司网上期货信息系统技术指引（中期协字〔2009〕66号）；
- 证券期货经营机构信息系统备份能力标准（JR/T 0059—2010）；
- 证券期货业信息系统安全等级保护基本要求（试行）（JR/T 0060—2010）；
- 证券期货业信息系统安全等级保护测评要求（试行）（JR/T 0067—2011）；
- 证券期货业信息系统运维管理规范（JR/T 0099—2012）。

五. 期货公司安全架构设计

5.1 网络结构规划

当前网络安全防护体系设计需要包含网络与信息安全风险检测、监测、评估和预警机制，发现风险隐患并能及时处置。具体网络结构如下图：



标注：

：防火墙系统　　ADS：抗拒绝服务系统　　IPS：网络入侵防御系统　　IDS：网络入侵检测系统

RSAS：远程安全评估系统（漏洞扫描）　　SAS-H：堡垒机系统　　DAS：数据库审计系统　　BVS：安全配置核查系统

5.2 指导思想

贯彻落实党中央“加强金融基础设施建设，保障金融市场安全高效运行和整体稳定”的要求，紧密围绕“确保资本市场平稳安全运行、有序健康发展”这个核心，密切结合行业信息化工作，推进落实《资本市场信息化建设总体规划(2014-2020)》和《金融业网络安全规划（2015-2020）》，加强证券期货业信息安全基础设施建设，稳步提升证券期货业信息安全保障水平，为监管转型、业务发展提供有力支撑，切实保护投资者权益。

对一个期货行业来说，各业务的重要程度应能很方便的进行区分。信息系统的建设应根据各业务的不同重要性，划分多个具有不同安全保护等级的安全域，实现不同强度的安全保护，具体包括的内容如下：

1. 重点保护思想：在分区域保护原则基础上，对于其中某些应用由于其处理、存储或传输的信息的性质，或者由于其对机构完成任务使命非常关键，需得到重点的保护；应集中资源首先确保重点应用安全，安全需求高安全域的重要应用应优先实施保护。

2.共同的安全需求的思想：安全域内的系统应具有相同或者相近的保护等级，实施统一的安全策略管理；

3.建立责任明确、保障有力的证券期货业信息安全治理体系，健全信息技术治理机制，提升信息安全地位，突出顶层设计能力；

4.加强行业信息安全公共基础设施建设，促进资源整合和安全服务共享，提升信息安全风险管理水平；

5.大幅提高信息系统风险防范能力和重大网络攻击抵御能力；

6.健全行业信息安全监管体系，提升监管效能，形成适应资本市场发展的监管机制；

7.提升信息技术安全可控水平，增强应急响应能力，保障行业信息系统的安全稳定运行。

5.3 具体防范思路

5.3.1 报盘区

期货公司与中金所、大商所、上期所、郑商所四家交易所以及开展业务，交易、查询及行情等主要业务都是通过此区域线路实现的，四家交易所相对属于可信区域，从信息安全角度来说，建设时应充分考虑以下内容：

- 链路冗余：建设时应充分考虑链路冗余机制，以便能够有效因某一运营商链路故障引发的网络中断；
- 安全逻辑隔离：边界应建立防火墙进行逻辑隔离，利用防火墙系统实现期货公司与四家交易所以及保证金中心进行逻辑隔离，对进出IP地址、端口等进行严格控制。

5.3.2 银期前置区

银期前置区放置的服务器系统旨在实现银行与期货公司之间的业务连接，为期货投资者提供资金转账服务，实现资金在本人银行结算账户与期货保证金账户之间定向实时划转。银行、期货公司分别通过各自渠道为客户提供查询服务。

在银期前置区边界建立防火墙，利用防火墙系统实现区域的隔离，从而限制了局部重点或敏感网络安全问题对全局网络造成的影响

5.3.3 广域网接入区

广域网接入区由广域网银期区、广域网客户服务区、广域网内联区组成，该区域的网络一旦出现异常，导致的将是业务中断，为此进行网络结构设计过程中需要根据具体处理业务的不同以及应用范围等情况，可以按照业务服务进一步划分安全子域，需要对其进行深入的调研分析后，根据安全域划分原则开展进一步的安全域规划。

对边界防火墙对的安全策略进行优化，安全策略应细化到IP地址和服务端口，以规范数据流的走向，实现业务安全访问。

5.3.4 客户托管交易前置区

该区域主要负责客户托管交易，该系统的安全性将关系到客户托管交易能否成功，从安全角度考虑，增加防火墙系统作为安全域边界防控隔离。

5.3.5 核心交换区

在期货公司网络系统的核心交换区，建议采用如下安全防护措施：

1) 对核心交换机器设备进行安全加固；

2)合理划分VLAN：根据其他安全域所承担的业务功能的不同，在核心交换机上划分相应的VLAN，并根据其业务通信流的需要设置相应的VLAN间路由策略和ACL访问控制策略。

3)IP、MAC、交换机端口绑定：在核心交换机上将重要主机和设备的IP地址、MAC地址、交换机端口进行绑定。

4)部署网络入侵检测系统：在核心交换机上部署基于网络的入侵检测系统，对通过此交换机中的网络流量中存在的攻击行为进行检测和分析，同时制定有序的监控策略，实现全维度监控，以有效的避免监控死角带来的隐患。

5.3.6 异地数据中心区

为了保障数据的安全，需要建立对应的数据中心，根据情况可考虑建立“同城灾备”、“两地三中心”等模式，由于双中心或三中心具备基本等同的业务处理能力并通过高速链路实时同步数据，日常情况下可同时分担业务及管理系统的运行，并可切换运行；灾难情况下可在基本不丢失数据的情况下进行灾备应急切换，保持业务连续运行。

5.3.7 互联网交易区

互联网交易区为整个期货公司唯一具备互联网出口的访问通道，出口要求具备双链路的前提下，需要增加必要的安全防护系统。为此在该区域增加专业的抗拒绝服务系统（ANTI-DDOS）实现对网络层攻击（SYN Flood，SYN-ACK Flood，ACK Flood，FIN/RST Flood ，UDP Flood，ICMP Flood，IP Fragment Flood、Stream flood等）以及应用层DDOS（HTTP get /post flood 攻击，慢速攻击，TCP连接耗尽攻击，TCP空连接攻击等）流量实现清洗；由于当前攻击方式、攻击类型极为繁多，建立在互联网交易区增加防火墙的基础上，应部署网络入侵防御系统（NIPS）以实现对应用层攻击进行拦截，更为重要的是利用网络入侵防御系统（NIPS）流式技术对网络中传送的文件，进行快速检测，比对文件信誉，对发现恶意的文件进行告警和阻断，同时还能够将恶意文件进行还原保存，用于恶意行为分析，还可以实现取证调查工作。

由于该区域是整个期货公司中安全事件高发区域，防护的同时应增加对数据库（DATABASE）系统的异常操作行为进行追踪、取证、分析。

5.3.8 运维管理中心区

运维管理中心区域一直是安全运维管理的核心区域，该区域的具备对整个网络的运维操作、管控权限，安全一旦“失手”将导致整个网络的“沦陷”。为此，应建立一台专门的安全管理服务器实现对网络中部署的全部安全系统实现集中、统一管控；增加漏洞扫描系统实现常态化的漏洞监控机制，以降低安全漏洞对应用系统构成的安全隐患；由于网络较为庞大，需要管理的各类主机、网络设备、安全设备较多，建议增加专业的安全运维管控系统即堡垒机，通过堡垒机系统可以帮助期货公司建立面向用户的集中、有序、主动的运维安全管控平台，通过基于唯一身份标识的集中账号与访问控制策略，与各服务器、网络设备等无缝连接，实现集中精细化运维操作管控与审计，降低人为安全风险，避免安全损失，满足合规要求，保障期货公司效益。

在后续的安全建设过程中，可以利用该区域管理服务器、安全设备所捕获的各位告警分析数据以及外部云安全平台可以形成一个完善的安全态势感知，通过态势感知平台可以快速、准确了解当前网络安装状况。

5.3.9 系统监控中心区

系统监控中心主要负责期货交易时间段的交易监控，在该中心区采取的边界防控为防火墙系统实现区域的逻辑隔离。该区域的组网模式与其他安全域的模式一致，均需采用冗余链路以及冗余主机系统。

四. 期货业建设参考的规范及要求

在期货公司IT架构设计的过程中，需要充分考虑规划对象系统的具体应用属性的同时应充分调研期货公司现网的技术风险、管理风险、制定和完善信息技术风险以及管理管理风险需要的安全防范思路，从而能够更好的优化信息技术基础架构、数据架构、应用架构、安全架构，提高信息技术系统的可用性、灵活性和可扩展性，以满足业务高速发展的需要。

同时，应推动期货业开展信息安全意识教育和安全技能培训，提高信息安全管理的专业化程度与安全防范意识。加强以数据安全为核心的防护体系建设，提升行业机构对重大网络攻击的响应和处置能力以及提高行业对安全管控水平。

参考文献：

1. 证券期货业信息系统安全等级保护基本要求（试行）（JR/T 0060—2010）；

2.期货公司信息技术管理指引（中期协字〔2014〕75号）；

3.《期货网上交易系统网络安全架构设计》王溢策 浙商期货有限公司 技术部；

4.《中国证券期货业信息安全工作规划》证券期货业信息化工作领导小组办公室 2014年11月；

5.http://finance.qq.com/a/20160316/006405.htm

6.http://blog.sina.com.cn/s/blog_15895af8d0102x8kq.html

浅析DDOS攻防

文/绿盟科技金融事业部 高级安全顾问 孙德福

现如今，信息技术的发展为人们带来了诸多便利，无论是个人社交行为，还是商业活动都开始离不开网络了。但是网际空间带来了机遇的同时，也带来了威胁，其中DDoS就是最具破坏力的攻击，通过这些年的不断发展，它已经成为不同组织和个人的攻击，用于网络中的勒索、报复，甚至网络战争。

什么是拒绝服务攻击(DOS)

DoS是Denial of Service的简称，即拒绝服务，造成DoS的攻击行为被称为DoS攻击，其目的是使计算机或网络无法提供正常的服务。最常见的DoS攻击有计算机网络带宽攻击和连通性攻击。带宽攻击指以极大的通信量冲击网络，使得所有可用网络资源都被消耗殆尽，最后导致合法的用户请求就无法通过。连通性攻击指用大量的连接请求冲击计算机，使得所有可用的操作系统资源都被消耗殆尽，最终计算机无法再处理合法用户的请求。

什么是分布式拒绝服务攻击(DDOS)

分布式拒绝服务(DDoS:Distributed Denial of Service)攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DoS攻击，从而成倍地提高拒绝服务攻击的威力。

DDOS 分类

在讲防御之前简单介绍一下各类攻击，因为DDOS是一类攻击而并不是一种攻击，并且DDOS的防御是一个可以做到相对自动化但做不到绝对自动化的过程，很多演进的攻击方式自动化不一定能识别，还是需要进一步的专家肉眼判断。

在讲防御之前简单介绍一下各类攻击，因为DDOS是一类攻击而并不是一种攻击，并且DDOS的防御是一个可以做到相对自动化但做不到绝对自动化的过程，很多演进的攻击方式自动化不一定能识别，还是需要进一步的专家肉眼判断。

网络层攻击

Syn-flood

利用TCP建立连接时3次握手的“漏洞”，通过原始套接字发送源地址虚假的SYN报文，使目标主机永远无法完成3次握手，占满了系统的协议栈队列，资源得不到释放，进而拒绝服务，是互联网中最主要的DDOS攻击形式之一。

ACK-flood

对于虚假的ACK包，目标设备会直接回复RST包丢弃连接，所以伤害值远不如syn-flood。DDOS的一种原始方式。

UDP-flood

使用原始套接字伪造大量虚假源地址的UDP包，目前以DNS协议为主。

ICMP-flood

Ping洪水，短时间内向目的主机发送大量ping包，造成网络堵塞或主机资源耗尽。比较古老的方式。

Land-based

攻击者将一个包的源地址和目的地址都设置为目标主机的地址，然后将该包通过IP欺骗的方式发送给被攻击主机，这种包可以造成被攻击主机因试图与自己建立连接而陷入死循环，从而很大程度地降低了系统性能。

应用层攻击

CC

ChallengeCollapsar的名字源于挑战国内知名安全厂商绿盟的抗DDOS设备-“黑洞”，通过botnet的傀儡主机或寻找匿名代理服务器，向目标发起大量真实的http请求，最终消耗掉大量的并发资源，拖慢整个网站甚至彻底拒绝服务。

DNS flood

伪造源地址的海量DNS请求，用于是淹没目标的DNS服务器。对于攻击特定企业权威DNS的场景，可以将源地址设置为各大ISP DNS服务器的ip地址以突破白名单限制，将查询的内容改为针对目标企业的域名做随机化处理，当查询无法命中缓存时，服务器负载会进一步增大。

慢速连接攻击

针对http协议，以知名的slowloris攻击为起源：先建立http连接，设置一个较大的content-length，每次只发送很少的字节，让服务器一直以为http头部没有传输完成，这样的连接一多很快就会出现连接耗尽。目前出现了一些变种，http慢速的post请求和慢速的read请求都是基于相同的原理。

系统漏洞性攻击

有些服务器程序存在bug、安全漏洞，或架构性缺陷，攻击者可以通过构造的畸形请求发送给服务器，服务器因不能正确处理恶意请求而陷入僵死状态，导致拒绝服务。例如某些版本的app服务器程序存在缓冲区溢出，漏洞可以触发但无法得到shell，攻击者可以改变程序执行流程使其跳转到空指针或无法处理的地址，用户态的错误会导致进程挂起，如果错误不能被内核回收则可能使系统当掉。

DDOS攻击方式

慢速连接攻击

针对http协议，以知名的slowloris攻击为起源：先建立http连接，设置一个较大的content-length，每次只发送很少的字节，让服务器一直以为http头部没有传输完成，这样的连接一多很快就会出现连接耗尽。目前出现了一些变种，http慢速的post请求和慢速的read请求都是基于相同的原理。

系统漏洞性攻击

有些服务器程序存在bug、安全漏洞，或架构性缺陷，攻击者可以通过构造的畸形请求发送给服务器，服务器因不能正确处理恶意请求而陷入僵死状态，导致拒绝服务。例如某些版本的app服务器程序存在缓冲区溢出，漏洞可以触发但无法得到shell，攻击者可以改变程序执行流程使其跳转到空指针或无法处理的地址，用户态的错误会导致进程挂起，如果错误不能被内核回收则可能使系统当掉。

混合型

在实际大流量的攻击中，通常并不是以上述一种数据类型来攻击，往往是混杂了TCP和UDP流量，网络层和应用层攻击同时进行。

反射型

反射型攻击的本质是利用“质询-应答”式协议，将质询包的源地址通过原始套接字伪造设置为目标地址，则应答的“回包”都被发送至目标，如果回包体积比较大或协议支持递归效果，攻击流量会被放大，成为一种高性价比的流量型攻击。反射型攻击利用的协议目前包括NTP、Chargen、SSDP、DNS、RPC portmap等等。

流量放大型

以上面提到的DRDOS中常见的SSDP协议为例，攻击者将Search type设置为ALL，搜索所有可用的设备和服务，这种递归效果产生的放大倍数是非常大的，攻击者只需要以较小的伪造源地址的查询流量就可以制造出几十甚至上百倍的应答流量发送至目标。

脉冲型

很多攻击持续的时间非常短，通常5分钟以内，流量图上表现为突刺状的脉冲。之所以这样的攻击流行是因为“打-打-停-停”的效果最好，刚触发防御阈值，防御机制开始生效攻击就停了，周而复始。蚊子不叮你，却在耳边飞，刚开灯想打它就跑没影了，当你刚关灯它又来了，你就没法睡觉。

链路泛洪

随着DDOS攻击技术的发展，又出现了一种新型的攻击方式link-flooding attack，这种方式不直接攻击目标而是以堵塞目标网络的上一级链路为目的。对于使用了ip anycast的企业网络来说，常规的DDOS攻击流量会被“分摊”到不同地址的基础设施，这样能有效缓解大流量攻击，所以攻击者发明了一种新方法，攻击至目标网络traceroute的倒数第二跳，即上联路由，致使链路拥塞。国内ISP目前未开放anycast，所以这种攻击方式的必要性有待观望。对一级ISP和IXP的攻击都可以使链路拥塞。[1]

DDOS防护

DDOS分层防护技术

ISP清洗：

当客户某核心业务遭受大规模DDOS攻击的时候，可以求助上级ISP进行流量清洗。一般分为两类：

ISP近源清洗：

绝大多数最终客户来说是不可见的，ISP运用自身强大的现网资源，先进的流量识别分析技术，大量的数据来源，判断是否将流量黑洞掉。

ISP近目的清洗：

对很多大型单位单位来说是必备的服务，其目的就是当客户某核心业务遭受大规模DDOS攻击的时候，可以求助上级ISP进行流量清洗。

CDN负载均衡：

可以理解为云清洗服务，是第三方流量清洗服务商为客户提供的“上游”DDOS清洗服务。其实现方式是预先设定好网站的CNAME， 并将域名指向这些服务商的DNS服务器，进行流量清洗，和流量回注，本质上说，这种方式并不是DDOS防护产品，但对于WEB类业务而言，恰恰具备一定的防护能力。

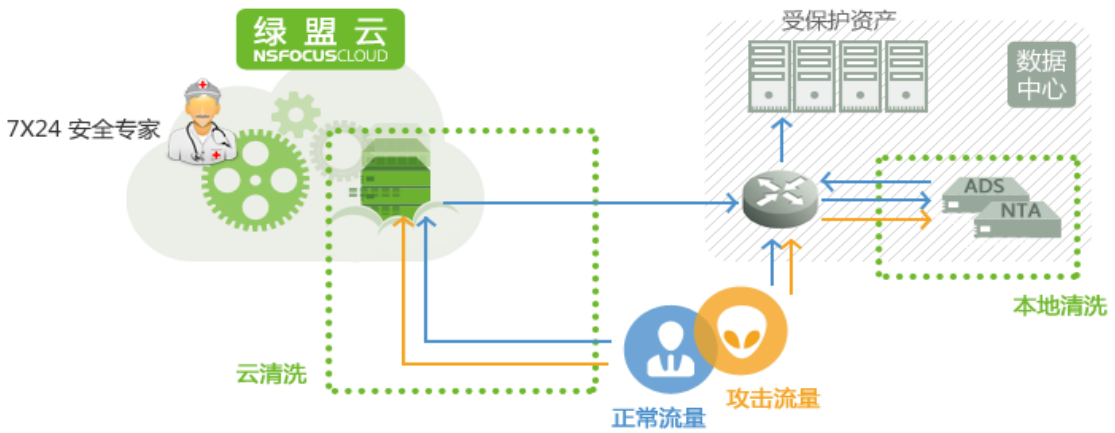
本地DDOS防御：

在数据中心本地还需要进行防护是因为ISP防护往往是粗暴的，不区分请求源真实性的，这就导致很多正常用户的请求也被拦截，同时小流量的防护通过本地抗DDOS设备防护，效果和成本相对更合算，对透过CDN防护到达源站的动态请求无法进行有效防护的这类场景，也需要在本地进行防护。

服务端DDOS防御策略：

通过做链路均衡、本地服务器的负载均衡，提高出口带宽，提高自身系统的健壮性。

绿盟科技综合抗DDOS服务



- 本地清洗

  智能防御算法，精确识别和防御DDos攻击

  防护各类已知和未知的DDos攻击，有效应对中小规模，复杂流量攻击

  自动清洗，在发现攻击时会自动进行流量牵引和清洗

  安全专家团队全天候远程值守

◆云端清洗

海量清洗，最高300Gbps云端防护能力

电信，联通双链路清洗

支持TCP/UDP/HTTP/HTTPS

适合金融、电商、游戏、门户、媒体等各类业务场景

◆ 优势

全面防御：本地＋云端，全面对抗DDos攻击，免于封IP，业务不再受影响

性价比高：不改变现有的网络结构，免安装，免部署，免维护

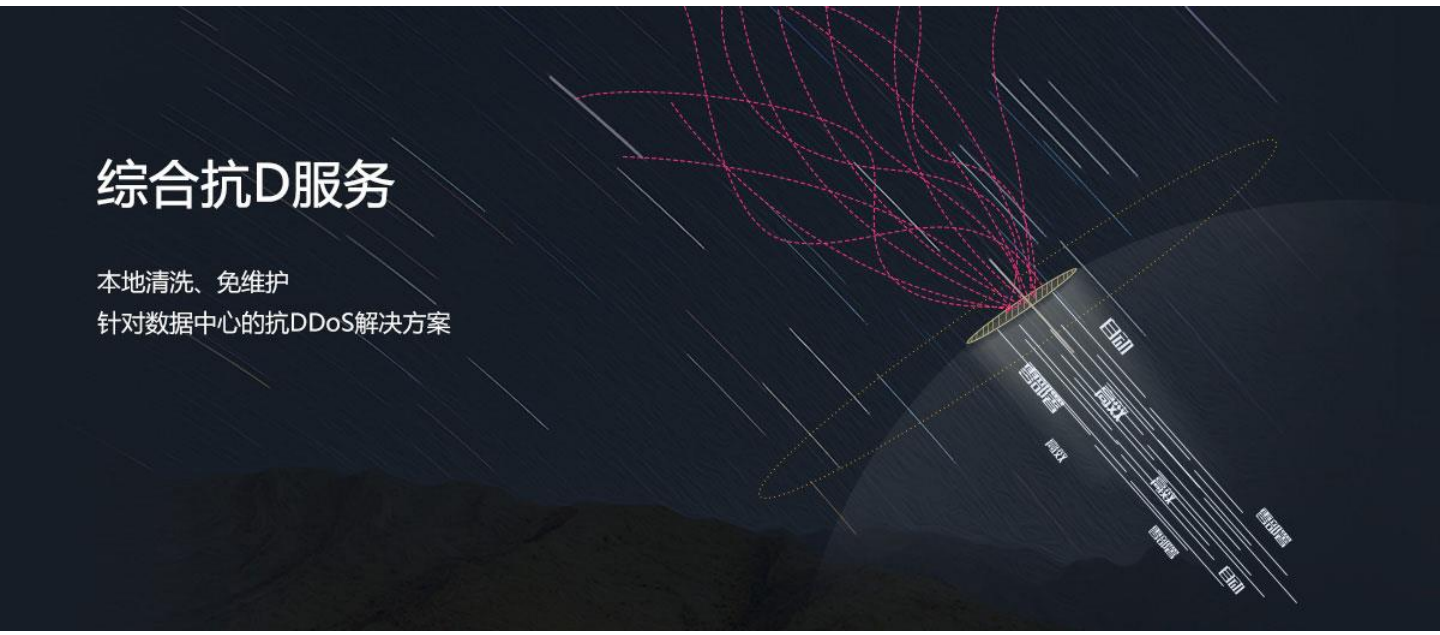
响应速度快：安全专家团队全天候远程守候

超乎寻常的稳定：本地清洗旁路部署，发现攻击时进行牵引，其他流量不受影响

成熟经验：15年抗DDos产品和流量清洗经验，帮助国内外客户建设，运营数百个清洗中心，国内唯一一家能够面向全行业用户提供抗拒服务攻击解决方案的专业厂商。

参考文献：

http://www.freebuf.com/articles/network/78660.html



Odinaff木马是土耳其金融攻击幕后黑手

拥有14000名员工的土耳其著名的最大上市银行之一Akbank最近遭到了Odinaff木马的攻击，其伎俩可能与之前曝光的Carbanak类似。

据卡巴斯基实验室报告：Carbanak跨国黑客团体专门针对全球约30个国家的银行和金融企业发起网络攻击并盗取银行账户资金，迄今所窃总金 高达10亿美元，受害国家和地区包括美国、欧盟、日本和中国等。这被认为是全球银行业迄今涉案金额最高、波及范围最广的“网络盗窃行为”之一。

虽然到目前为止细节尚未公开，但是从仅有的公布细节看，遭受攻击主要原因是其员工遭到了钓鱼邮件的攻击，采用的是传统的DOC文档中嵌入了恶意宏的方式。

到这里为止还没看出什么特别的地方。但是后续的动作有点值得关注了：该木马并没有急于全线开火，而是先用上一些无害或者轻量的武器比如进程查看工具Psexec,网络扫描工具Netscan，免费的远程桌面工具软件Ammyy以及轻量级的Windows系统密码神器Mimikatz等。之所以这样做，就是为了麻痹一些普通的安全防线：因为这些防护系统大多会扫描和检查大多数的未知以及新出现的文件。攻击者收集信用卡信息，并通过SWIFT系统执行汇款，并执行一些其他恶意操作。

据悉还有两家土耳其银行遭受攻击，但并未对外发布声明或其他信息。

该木马大部分的攻击目标是在金融领域，小部分的对象是证券、法律、卫生和健康以及政府部门。

来源：
http://securityaffairs.co/wordpress/54495/malware/odinaff-attack.html
http://bbs.antiy.cn/forum.php?mod=viewthread&tid=76087

攻击乌克兰电网的黑客组织变身TeleBots攻击乌克兰银行

一年前， BlackEnergy黑客组织对乌克兰电网发起网络攻击，而这次BlackEnergy变身为“TeleBots”组织攻击乌克兰银行。

“黑暗力量”（BlackEnergy）组织一年前攻击乌克兰电网，导致乌克兰大规模停电。乌克兰政府指责俄罗斯参与其中，但进一步的分析表明，BlackEnergy恶意软件并不是乌克兰断电的直接原因。

ESET公司的专家表示，BlackEnergy黑客组织正利用TeleBots恶意软件攻击乌克兰银行。TeleBots恶意代码与BlackEnergy组织使用的恶意软件有许多相似之处。ESET推测，BlackEnergy已经演变为TeleBots组织。ESET发表博文称，“2016年下半年，ESET研究人员识别出一款独特的恶意工具集，针对乌克兰金融行业的高价值目标实施网络攻击。我们认为，攻击者使用这些工具的主要目标是进行网络破坏。本篇博文概述了此次网络活动的细节。”

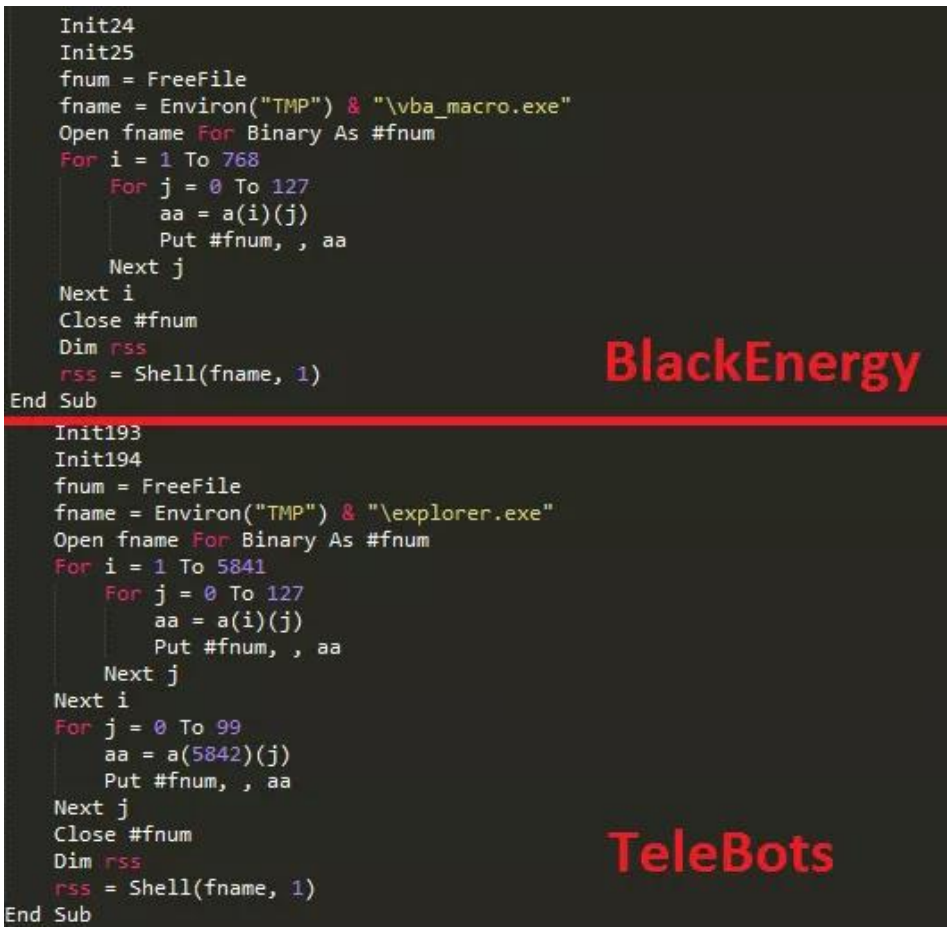
“我们将提到恶意软件TeleBots背后的团伙。然而，这些攻击者及其使用的工具集与BlackEnergy黑客组织存在众多相似之处。BlackEnergy 2015年12月与2016年1月曾对乌克兰的能源行业发起网络攻击。事实上，我们认为BlackEnergy组织已经变身TeleBots组织。”

黑客通过包含恶意宏的Microsoft Excel文档利用鱼叉式网络钓鱼信息攻击受害者。

一旦受害者点击“启用内容”（Enable Content）按钮，TeleBots文档中的宏通过使用explorer.exe文件名释放恶意二进制并执行二进制。其恶意代码为木马下载器，通过Rust程序语言编写，负责下载并执行另一种恶意软件。

ESET表示，“一旦受害者点击Enable Content按钮，Excel执行恶意宏。我们的分析表明，TeleBots文档中使用的宏代码与BlackEnergy黑客组织2015年使用的相匹配。”

以下为BlackEnergy与TelBots源代码的相似之处：



“宏的主要目的是利用explorer.exe文件名释放恶意二进制，之后执行二进制。释放的二进制属于木马下载器家族，旨在下载并执行另一恶意软件。这个目标下载器用Rust程序语言编写。”

TeleBots黑客能完全劫持设备并在目标网络加以扩散。专家注意到，该组织还能在目标设备上植入KillDisk恶意软件，使目标设备显示FSociety Mr Robot（《黑客军团》地下黑客组织FSociety）为主题的标识之前无法启动。

专家肯定，TeleBots威胁攻击者旨在实施网络破坏攻击。很显然，俄罗斯是头号嫌疑。

来源：

https://www.easyaq.com/newsdetail/id/760819983.shtml

Odinaff木马是土耳其金融攻击幕后黑手

卡巴斯基实验室专家发现了Faketoken手机银行木马的一种变种，该变种能够加密用户数据。这种恶意程序会伪装成多种程序或游戏，包括Adobe Flash Player，窃取超过2,000种安卓金融应用的登陆凭证。截止到目前，这种Faketoken变种已经在27个国家造成超过16,000名受害者感染，其中大多数用户都位于俄罗斯、乌克兰、德国和泰国。

新增的数据加密功能对木马程序来说并不常见，因为大多手机勒索软件主要是拦截用户使用设备，而非锁定数据，而且用户的数据通常会备份到云端。在Faketoken攻击中，用户的数据，包括文档和媒体文件如照片和视频都会利用一种AES对称加密算法进行加密。有些情况下，用户可以不必向网络罪犯支付赎金而解密这些数据。

在感染初始阶段，木马会要求管理员权限，还要求用户同意该木马覆盖其他应用，或者成为默认的短信应用。通常情况下，用户几乎没有其他选择，只能选择同意。此外，这些权限还让Faektoken木马能够窃取数据，而且不仅能够直接窃取如联系人和文件等数据，还能够利用钓鱼网页，间接窃取其他数据。

该木马被用于在全球范围内窃取数据：一旦木马获取到所有请求的权限，就会从自己的命令和控制服务器数据库。数据库包含77种语言，适用于不同地区的多种设备。这些数据库被用于创建钓鱼信息，窃取用户的Gmail账户密码。此外，该木马还能够覆盖Google Play应用商店，显示一个钓鱼页面窃取用户的信用卡信息。事实上，这种木马能够下载一个包含很多可被攻击的应用列表，甚至利用HTML模板页面生成钓鱼页面，窃取相关应用的账户信息。卡巴斯基实验室的研究人员发现该列表中包含2,249种金融应用。

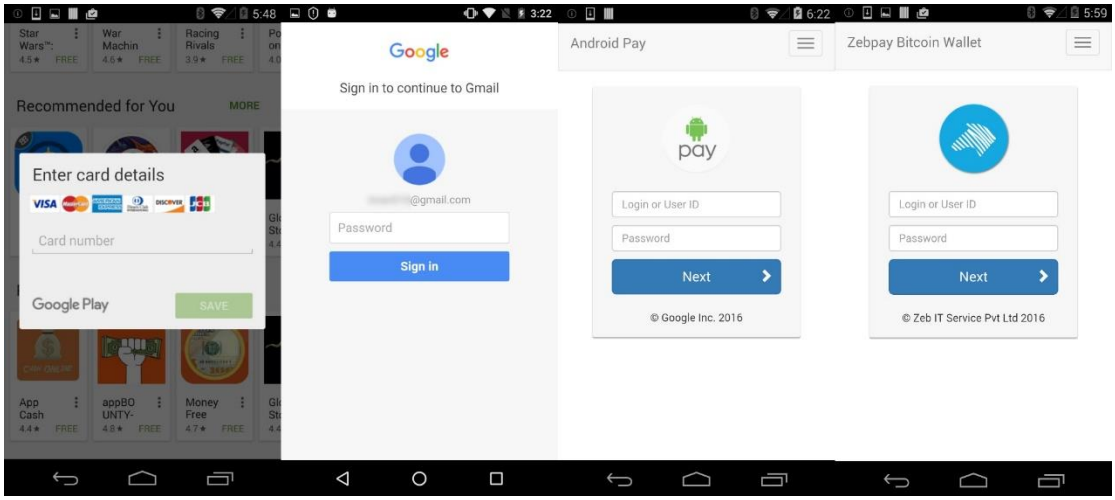
有趣的是，这种Faketoken变种还会利用自己的快捷方式替换社交媒体网络、即时通讯工具和浏览器的快捷方式。这样做的原因尚不明确，因为替换的图标仍然指向合法的应用程序。

卡巴斯基实验室高级恶意软件分析师Roman Unuchek说：“最新的Faketoken手机银行木马变种非常有趣，因为有些最新的功能似乎给攻击者带来的优势非常有限。但是，这并不意味着我们不应当慎重处理这种威胁。这些变化可能表示网络罪犯在为未来开发打基础，或者表明恶意软件在不断演化和创新。通过曝光这一威胁，我们能够消除它带来的威胁，帮助用户保护设备和数据安全”。

卡巴斯基实验室建议安卓用户采取以下措施保护自己的安全，抵御Faketoken木马和其他恶意软件威胁：

- 确保对所有的数据进行备份。
- 当一款应用要求权限时，不要轻易同意这些权限——请仔细思考一下这些应用要求的是什么权限，以及为什么要获取这些权限。
- 在所有的设备上安装反恶意软件解决方案，同时保持自己的操作系统和软件及时更新。

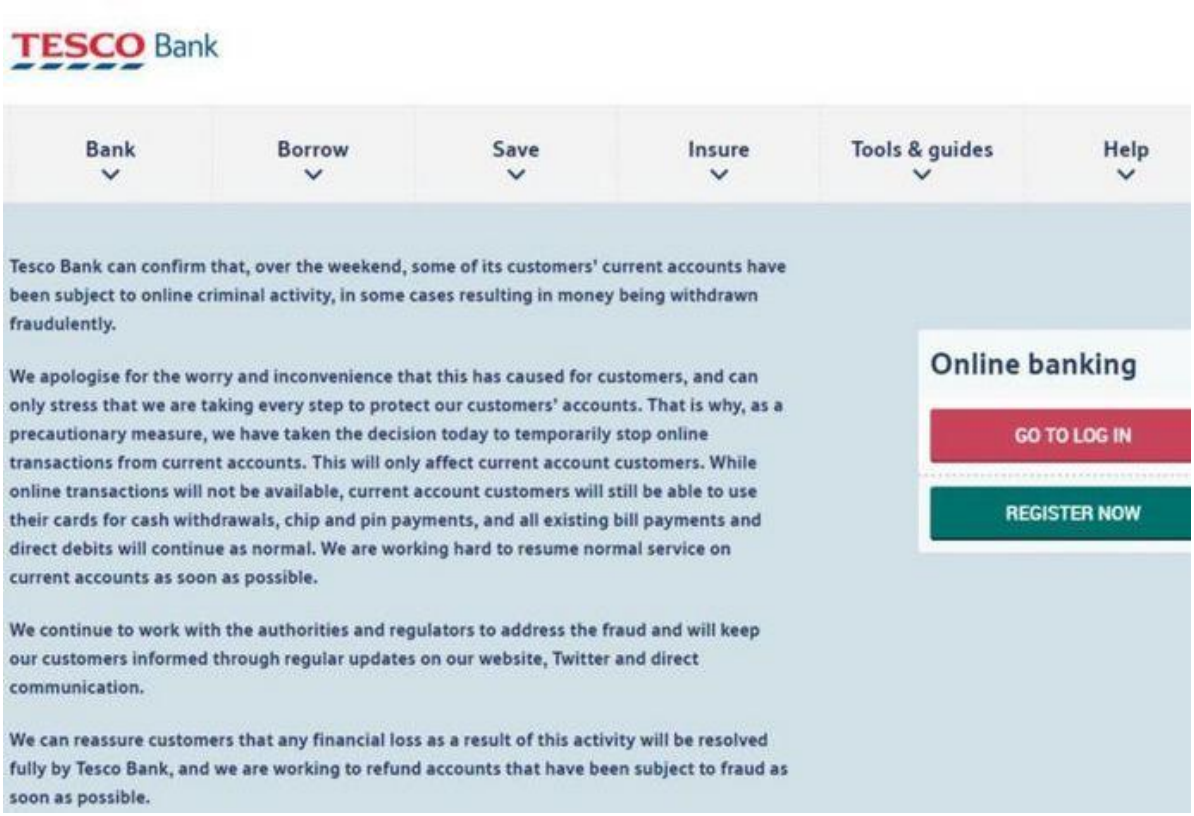
卡巴斯基实验室检测到数千个能够加密数据的Faketoken安装包，其中最早的可以追溯到2016年7月。卡巴斯基实验室产品能够检测Faketoken恶意软件家族的所有变种。



来源：

http://www.ithome.com/html/it/283631.htm

https://www.bleepingcomputer.com/news/security/its-now-commonplace-for-android-banking-trojans-to-include-ransomware-features/



此次事件发生的时间段是上周六深夜至周日凌晨，Tseco银行的反应很快，周日一早就通过短信来提醒用户他们的账号可能出现了问题，还提到如果需要更多的信息可以电话咨询。然而据银行blog上的情况可以想象，他们的客服中心应该很快就被电话打爆了，很多人在blog留言说自己打过去的电话没有人接。不过这些留言都还是以抱怨为主，并没有太多过激的言论。

有用户提到他的账户在他不知情的情况下就少了700磅；还有位母亲抱怨到因为服务中断她不能给自己家在外上学的小孩打钱了。

分管国家网络犯罪的英国国家犯罪处将会对这次被称为“Tesco银行数据泄露”的事件进行协调执法。而来自英国数据保护机构信息专员办公室的一位代表说，已经了解了此次事件并会开展进一步调查，期望能够发现更多细节。

新型针对ATM的恶意软件出现

摘要

来自Trend Micro公司的安全专家们已经发现了一种新型ATM恶意软件，这种被称为Alice的攻击机制旨在针对各类自助式服务ATM设备中的安全保护功能。

此恶意软件非常值得关注，它最大的特点就是不同于其它ATM恶意软件,因为其无法实现数据窃取功能，同时亦不可通过ATM数字键盘进行控制，Alice利用的是原有安全机制清空和实机操作取现。

研究人员们最初于2016年11月首次发现Alice ATM恶意软件，而这项工作为Trend Micro与Europol EC3建立的联合研究项目的一部分，不过他们推测此恶意软件的诞生时间应该在2014年。

在初次发现Alice时，研究人员们曾经怀疑其属于已知ATM恶意软件Padpin的新型变种。但经过进一步调查后，他们发现了Alice属于一种全新恶意软件家族。

与其它ATM恶意软件家族不同，Alice无法通过ATM的数字键盘进行控制，亦不包含任何信息窃取功能。其作用单纯只是清空ATM的现有安全保护功能。

根据研究人员的说法，诈骗分子需要以物理方式访问ATM以清空其分配器，这一迹象表明Alice的设计目标在于实现“钱骡”——即非法财产转移。

由于在进行资金转账前需要输入PIN码，因此可以认定Alice仅被用于进行现场攻击。Alice并不具备精心设计的安装或者卸载机制——其只能在适当环境中通过运行可执行文件实现功能

Alice ATM恶意软件还可通过远程桌面协议（简称RDP）实现运行，但研究人员们还没有发现任何存在此种使用方式的证据。

研究人员们注意到，该恶意软件只会接入CurrencyDispenser1外设且并不包含任何负责使用PIN数字键盘的代码，这可能是因为其设计目标在于帮助诈骗分子以物理方式使用ATM并利用USB或者光盘对其进行感染。

Alice支持通过特定PIN码执行以下三条命令：

- 删除一个文件以进行卸载。
- 退出该程序并运行卸载/清理程序。

•打开“操作面板”以查看ATM中的可用现金量。

在攻击场景下，该钱骡会输入目标ATM用于资金分检的钞匣ID，而出钞命令则通过WFSExecute API发送至CurrencyDispenser1外设处。

ATM设备通常设有最多40张出钞量上限，这意味着诈骗分子需要多次重复操作才能取空钞匣中的全部现金

Alice不具备长期运行的能力，因此攻击者需要手动将Windows任务管理器（taskmgr.exe）替换为Alice，意味着任何调用任务管理器的命令都会转而调用Alice。

来源

https://www.easyaq.com/newsdetail/id/1784343021.shtml

银行大劫案再袭：多国银行被盗损失惨重

摘要

继孟加拉后又一个国家央行遭遇惊天劫案。据CNNMoney2日报道，黑客入侵了俄罗斯央行并从该行的代理银行账户中偷走了20亿卢布（约合3100万美元）。该央行周五证实了这一消息。

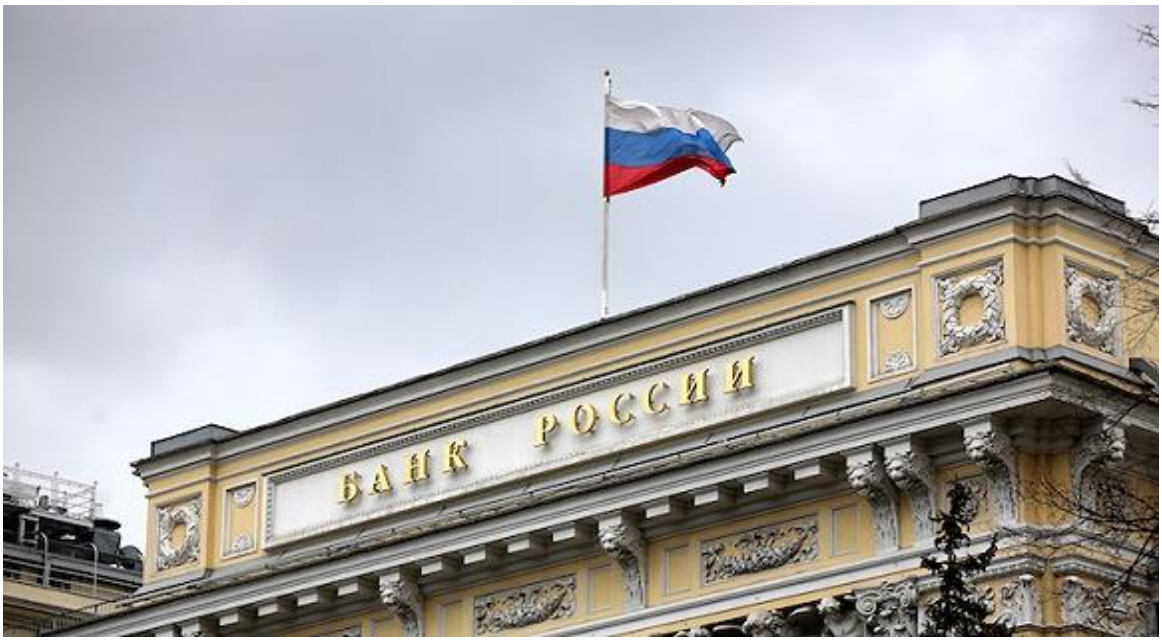
报道援引俄罗斯央行安全官员Artyom Sychyov的话说，黑客本来试图盗窃50亿卢布，但当局成功阻止了他们，将这笔资金转移到了它处。“我们很幸运的找回了部分资金，”一名央行发言人称。

央行没有指出这起黑客盗窃案是什么时候发生的，以及被窃资金是如何被转走的，不过报道称，截至目前，这起案子跟最近针对全球金融体系的一系列入侵事件有相似之处。

2015年1月，黑客通过SWIFT（环球同业银行金融电讯协会）获得了厄瓜多尔银行的代码，窃取了该行存在富国银行的资金。今年10月，黑客利用同样的手段潜入了菲律宾一家银行。两个月后，黑客入侵越南一家商业银行试图做出虚假操作指令但没有成功。

今年2月，孟加拉国央行纽约联储账户1.01亿美元资金被盗（其中2000万被追回），也是通过SWIFT平台实施的。

不过到底是谁入侵了俄罗斯央行还不明确。周五早些时候，政府宣称挫败了一起试图动摇公众对该国金融体系信心的阴谋。俄罗斯联邦安全局（FSB）称黑客计划利用位于荷兰的服务器来攻击俄罗斯银行。FSB还说，黑客还计划通过在社交媒体上伪造俄罗斯银行倒闭等消息，来扰乱该国的金融体系。



事件后续1：继俄罗斯央行被盗后，俄国有银行 VTB 遭 DDoS 攻击

俄罗斯最近正设法阻止一系列针对本土银行的网络攻击事件。据法新社报道，俄罗斯国有银行 VTB 网站近日遭到网络 DDoS 攻击，官方称 IT 基础设施仍然在正常工作、用户的账户不受攻击影响。

12 月 2 日俄罗斯联邦安全局(FSS)表示国外情报机构正策划一系列的网络攻击计划针对俄罗斯银行系统。俄罗斯联邦安全局已经成功挫败了一起拟于 12 月 5 日发动的攻击计划，攻击者的服务器属于乌克兰公司 BlazingFast、物理位置在荷兰。

事件后续2：土耳其 Akbank 银行SWIFT系统遭黑客入侵，或面临 400 万美元损失

据路透社报道，土耳其第三大上市银行 Akbank 的 SWIFT 系统遭黑客入侵，事件发生于 12 月 8 日，官方表示虽然攻击并未对 Akbank 的运营或财务产生影响，也没有造成客户数据泄露，但此次事件可能会导致 Akbank 银行面临 400 万美元的损失。所幸潜在损失或有保险公司负责支付。

事件后续3

SWIFT 已向各国银行致信，就日益严峻的黑客攻击活动向后者发出警告，提醒各家银行需对此提高警惕。

银行木马Dyre新变种悄然来袭亚太

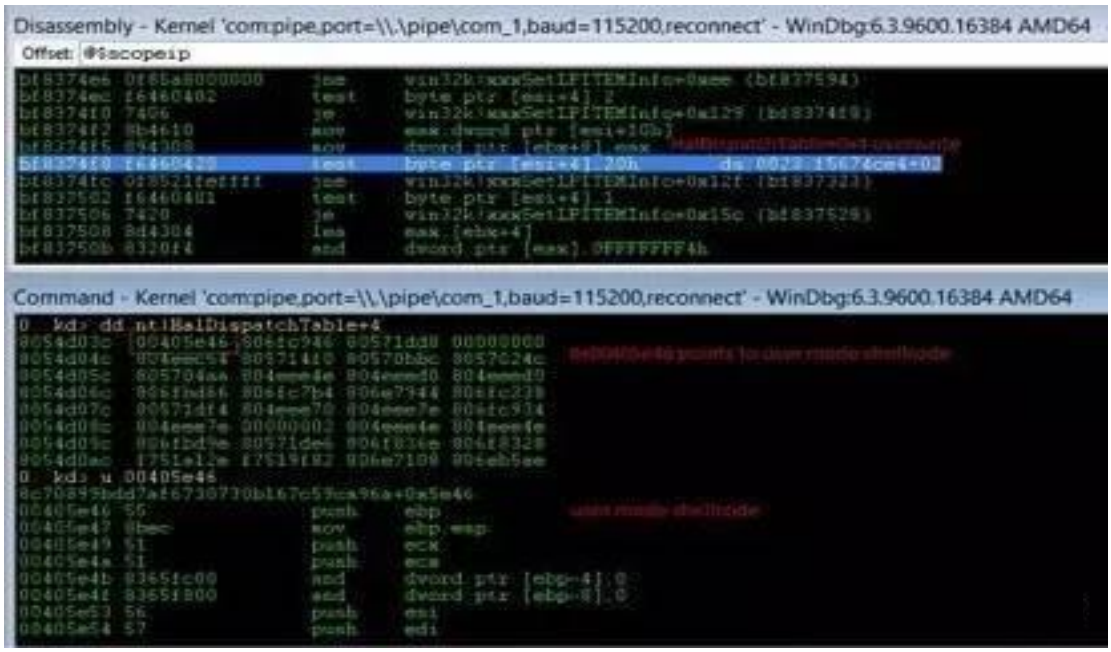
背景

2016年10月，目标为新加坡、印度和马来西亚的特洛伊木马TrickBot，被IBM X-force 安全研究人员证实与恶意代码Dyre相关。

特洛伊木马Dyre 是以前的目标是澳大利亚、英国、新西兰和德国，而同一伙黑客在TrickBot中增加了重定向攻击功能。

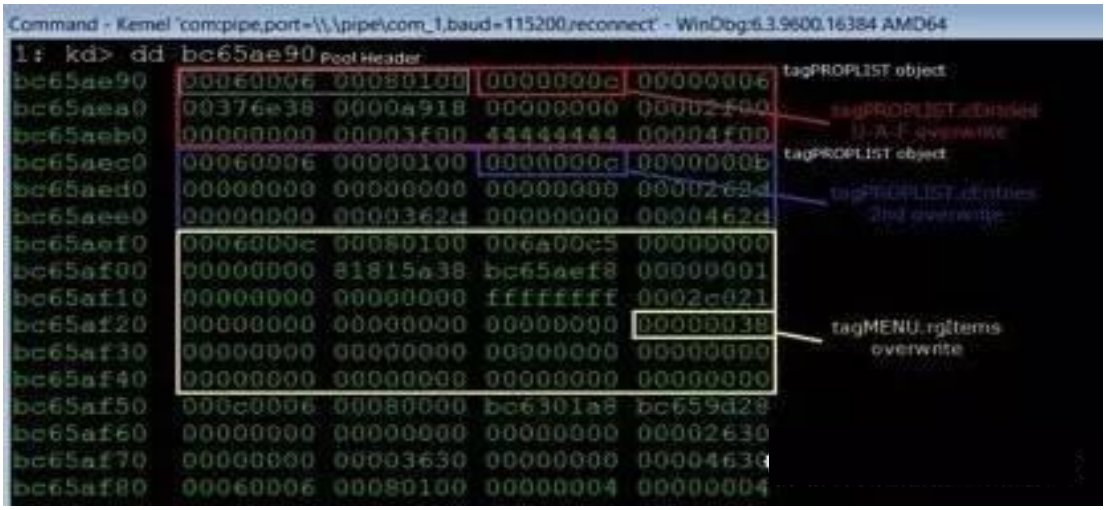
Dyre银行发展趋势之一

新变种利用了微软的Windows（CVE-2015-0057）一个修补漏洞。CVE-2015-0057是一个释放后使用漏洞自由存在于Windows内核，可以被利用来执行本地权限提升的Win32k.sys中的组成部分。除此之外,这些新变种Dyre还包括利用CVE-2013-3660作为后备,以防系统打补丁的CVE-2015-0057 。



Dyre银行发展趋势之二

木马Dyre（又称Dyreza）在经过最近的升级后，把目标瞄准了Win10的Edge浏览器，又被称为“网络犯罪雇佣”服务，主要作案目标为销售团队用户以及银行客户。Dyre将会抓取浏览器进程，并且通过提升权限来监控特殊范围内的连接，收集用户输入的凭据。这种攻击方式被称为“man in the browser”。一般来说，这种方式经常被利用来窃取用户与钱财有关的账户信息，比如网银、支付宝等、亚马逊等账号和密码等信息。IE11、Chrome、Firefox和Edge等浏览器都在其攻击范围。



TrickBot目前被发现在上述三个亚洲国家增长快速扩散。而TrickBot并不是首先面向新加坡的，它几乎是与Dyre、 Dridex、 Neverquest 和 Tinba，针对英语国家，沿着相似的路线扩散的。

TrickBot重点目标是业务账户、公司及商业银行和财富管理机构，在印度和马来西亚商业银行也是其主要目标，视乎它只对这些现金进出的相关者感兴趣。

TrickBot的重定向攻击会对58%的目标 Url 的进行。而其他木马的正在减少他们的重定向攻击或完全删除它们，例如：GozNym在某些地区减少其重定向攻击比率为12%或更低。在攻击中，网络犯罪人通过创建“令人信服”的假冒银行网站，欺骗用户进入（后续活动可想而知，你的用户凭证，呵呵了）。有些情形，甚至使用银行的URL 和安全套接字层 (SSL) 证书，使他们显得更令人信服。

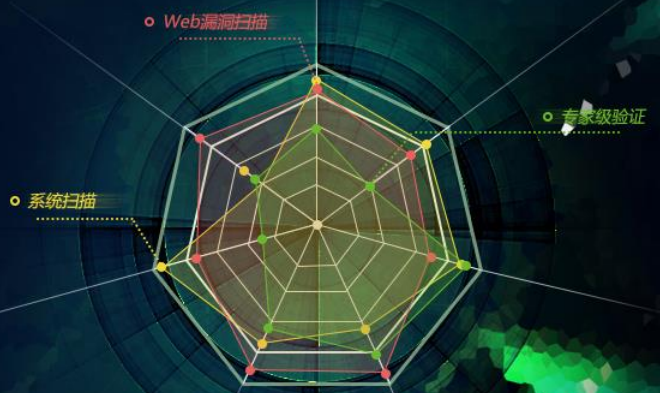
目前以银行等金融机构为目标的恶意软件正在快速增长，由于其背后的巨大经济利益，未来这种趋势将更为加速。而在目前的金融界，网络安全就是生产安全，万万不能忽视，金融界的网络安全同仁们小心喽~！

来源：微信公众号malwarebenchmark

绿盟云 NSFOCUS CLOUD

网站安全评估

支持系统和Web漏洞扫描
对高中危漏洞进行专家级验证



1 您的网站被黑了，黑客是如何攻击网站的？您的网站有哪些漏洞？

2 OpenSSL的“心脏滴血”漏洞，Apache Struts2的多个高危漏洞，以及Shell-shock漏洞，这些最近几年著名的安全漏洞，您的网站是不是还存在？

3 您的网站应用就要正式上线和运行了，需要客观的安全数据依据。

4 您的网站要进行信息系统安全等级保护定级和测评、要迎接上级的安全检查，需要进行漏洞扫描。

如果您有以上需求 我 可以快速且轻松地帮您解决

服务套餐	体验版	标准版（1次）	标准版（5次）	标准版（10次）
系统扫描	✔	✔	✔	✔
Web扫描	✔	✔	✔	✔
扫描报表	✔	✔	✔	✔
扫描次数	1次	1次	5次	10次
价格	¥0 / 年	¥500 / 年	¥2250 / 年	¥4000 / 年

cloud.nsfocus.com

NSFOCUS

漏洞聚焦

NSFOCUS

漏洞聚焦

Apache HTTPD拒绝服务漏洞安全威胁通告

综述

2016年12月5日（当地时间），seclists.org网站发布了一条关于Apache网页服务器拒绝服务漏洞的消息，漏洞编号为 CNNVD-201612-069 。 该漏洞存在于mod_http2模块中

这是从Apache HTTPD 2.4.17版本开始引入的关于HTTP/2协议的模块。然而该模块在默认情况下不被编译，且默认不启用，该漏洞只影响使用HTTP/2协议的用户。在使用HTTP/2协议的服务器上，攻击者可以通过发送精心构造的请求，导致服务器内存耗尽，造成拒绝服务。

相关链接地址如下：http://seclists.org/oss-sec/2016/q4/595

漏洞危害

成功利用漏洞后，耗尽服务器内存，导致拒绝服务攻击。

受影响的版本

- Apache HTTPD version 2.4.17
- Apache HTTPD version 2.4.17
- Apache HTTPD version 2.4.17
- Apache HTTPD version 2.4.17

不受影响的版本

无

什么是HTTP/2?

HTTP/2（超文本传输协议第2版，最初命名为HTTP 2.0），是HTTP协议的的第二个主要版本，使用于万维网。HTTP/2是HTTP协议自1999年HTTP 1.1发布后的首个更新，主要基于SPDY协议。它由互联网工程任务组（IETF）的Hypertext Transfer Protocol Bis（httpbis）工作小组进行开发。HTTP/2的目标包括异步连接复用，头压缩和请求反馈管线化并保留与HTTP 1.1的完全语义兼容。（引用自《维基百科》）

代码修复

github上已经对该漏洞进行了源代码修复，部分修复情况如下所示。

修复代码中增加了对h2_stream_add_header函数返回值重置状态的判断。

```
404  404      status = h2_stream_add_header(stream, (const char *)name, namelen,
405  405                                     (const char *)value, valuelen);
406       -    if (status != APR_SUCCESS && !h2_stream_is_ready(stream)) {
     406  +    if (status == APR_ECONNRESET) {
     407  +        ap_log_cerror(APLOG_MARK, APLOG_TRACE1, status, session->c,
     408  +                      "h2-stream(%ld-%d): on_header, reset stream",
     409  +                      session->id, stream->id);
     410  +        nghttp2_submit_rst_stream(ngh2, NGHTTP2_FLAG_NONE, stream->id,
     411  +                                  NGHTTP2_INTERNAL_ERROR);
     412  +    }
     413  +    else if (status != APR_SUCCESS && !h2_stream_is_ready(stream)) {
407  414          return NGHTTP2_ERR_TEMPORAL_CALLBACK_FAILURE;
408  415      }
409  416      return 0;
```

修复代码中修改了对已添加头部的检查，并且在条件不成立时，返回的状态为“重置连接”。

源代码修复地址如下：

https://github.com/apache/httpd/commit/29c63b786ae028d82405421585e91283c8fa0da3

```
358        -        if (name[0] != ':') {
359        -            ++stream->request_headers_added;
360        -            if (stream->request_headers_added
361        -                > stream->session->s->limit_req_fields) {
362        -                /* too many header lines */
363        -                ap_log_cerror(APLOG_MARK, APLOG_TRACE1, 0, stream->session->c,
364        -                              "h2_stream(%ld-%d): too many header lines",
365        -                              stream->session->id, stream->id);
366        -                return h2_stream_set_error(stream,
367        -                                           HTTP_REQUEST_HEADER_FIELDS_TOO_LARGE);
368        -            }
     351   +    }
     352   +    else if ((nlen + 2 + vlen) > stream->session->s->limit_req_fieldsize) {
     353   +        /* header too long */
     354   +        ap_log_cerror(APLOG_MARK, APLOG_TRACE1, 0, stream->session->c,
     355   +                      "h2_stream(%ld-%d): header %s too long",
     356   +                      stream->session->id, stream->id, name);
     357   +        error = HTTP_REQUEST_HEADER_FIELDS_TOO_LARGE;
     358   +    }
     359   +
     360   +    if (stream->request_headers_added
     361   +        > stream->session->s->limit_req_fields + 4) {
     362   +        /* too many header lines, include 4 pseudo headers */
     363   +        if (stream->request_headers_added
     364   +            > stream->session->s->limit_req_fields + 4 + 100) {
     365   +            /* yeah, right */
     366   +            return APR_ECONNRESET;
```

规避方案

Apache官方尚未发布版本更新，然而github上已经对该漏洞进行了源代码修复，建议用户下载最新的源码编译安装。github链接地址如下：

https://github.com/apache/httpd

作为临时的缓解策略，已经启用HTTP/2的用户也可以从配置文件的“Protocols”行中删除“h2”和“h2c”从而禁用HTTP/2 。

Firefox跨域设置cookie漏洞安全威胁通告

综述

2016年12月6日，insert-script.blogspot.gr网站发布了一条关于Firefox跨域设置cookie的消息，该漏洞的成因是火狐浏览器允许元标签对浏览器cookie进行设置。成功利用该漏洞会使得目标用户在跳转到恶意站点之后，对用户浏览器中的cookie进行设置。

相关链接地址如下：

https://insert-script.blogspot.gr/2016/12/firefox-svg-cross-domain-cookie.html

受影响的版本

- Mozilla Firefox version < 50.0.2

不受影响的版本

- Mozilla Firefox version < 50.0.2

规避方案

经过测试，火狐最新版本50.0.2不受该漏洞的影响，建议用户升级到不受影响的最新版本（50.0.2），下载页面如下：https://www.mozilla.org/en-US/firefox/products/

漏洞验证

对该漏洞的复现情况如下。

实验中，用户所访问的正常网站中，存在如下代码：

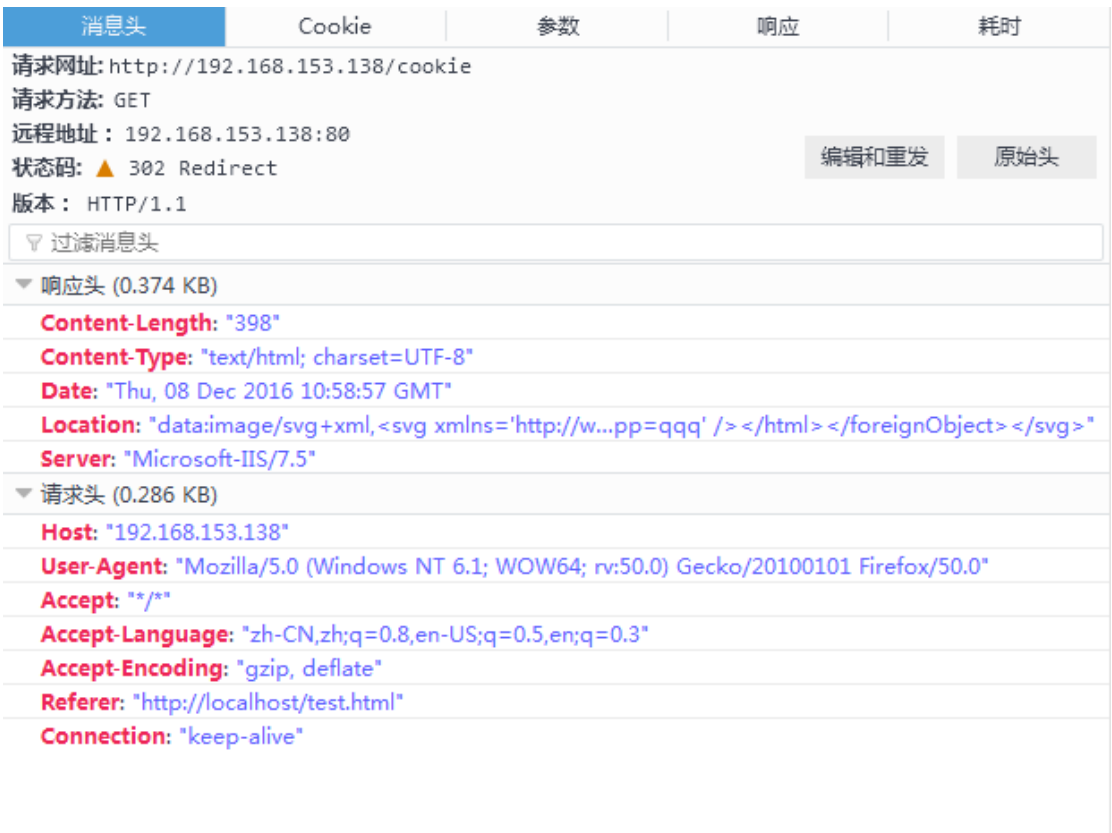
```
<!DOCTYPE html>
<html>
<head>
<title>SVG</title>
</head>
<body>
<img src="http://192.168.153.138/cookie">
</body>
</html>
```

其中，192.168.153.138为攻击者的网站。当用火狐浏览器访问上述网页时，浏览器会跳转到攻击者的网站去请求“http://192.168.153.138/cookie”资源，而攻击者的网站对该资源进行了重定向，并且在HTTP响应头Location中设置了攻击代码，如下图所示：

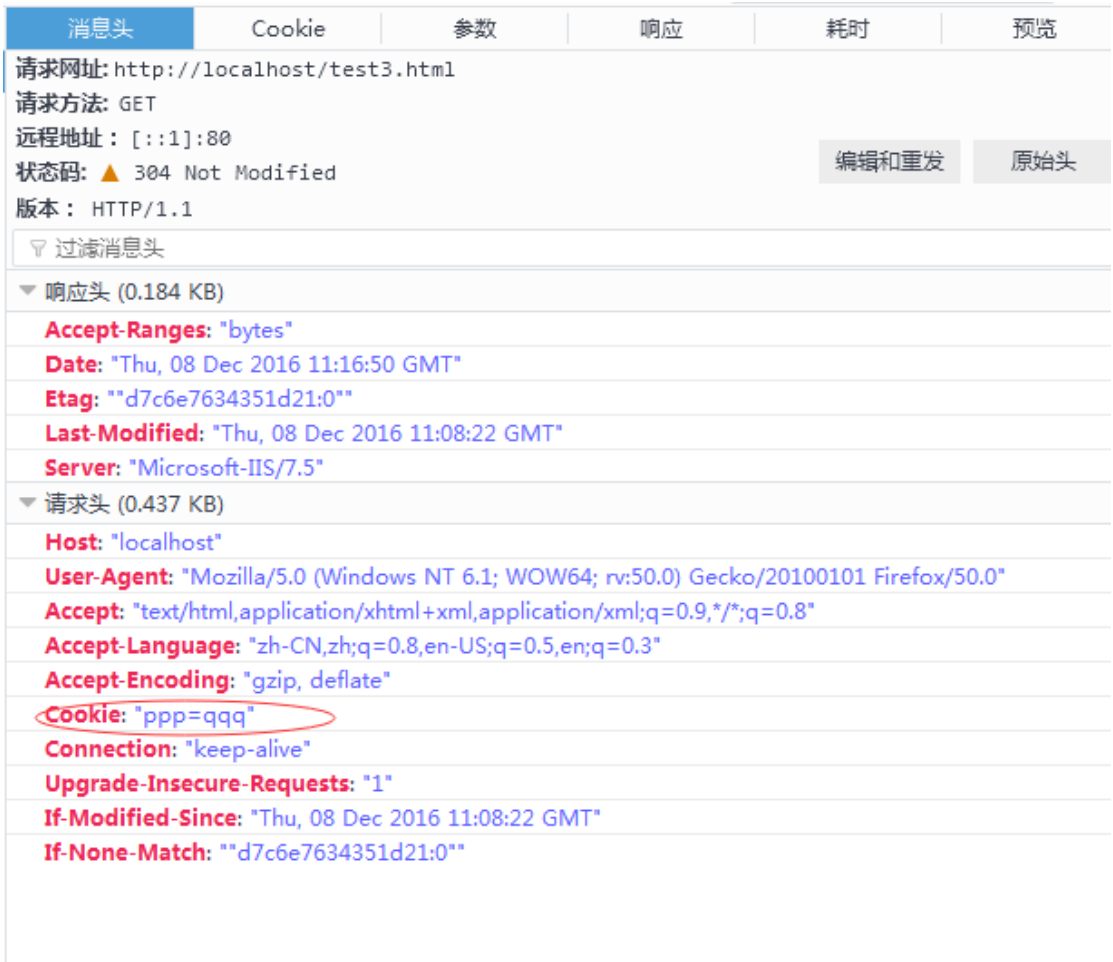
```
<svg xmlns='http://www.w3.org/2000/svg'>
<circle r='100'>
</circle>
<foreignObject>
<html xmlns='http://www.w3.org/1999/xhtml'>
<meta http-equiv='Set-Cookie' content='ppp=qqq' />
</html>
</foreignObject>
</svg>
```

由上图可知，攻击者准备的cookie为“ppp=qqq”。漏洞触发前，访问正常网站时并未携带cookie，如下图所示：

接下来，访问图1中的网页，浏览器会跳转到攻击者的网站，并被重定向，且返回的响应头Location中加入了攻击代码：



之后，再次访问正常网站时，浏览器已经带上了攻击者所准备的cookie：


消息头
Cookie
参数
响应
耗时
预览
请求网址: http://localhost/test3.html
请求方法: GET
远程地址： [::1]:80
状态码: 304 Not Modified
版本： HTTP/1.1
编辑和重发
原始头
过滤消息头
响应头 (0.184 KB)
Accept-Ranges: "bytes"
Date: "Thu, 08 Dec 2016 11:16:50 GMT"
Etag: ""d7c6e7634351d21:0""
Last-Modified: "Thu, 08 Dec 2016 11:08:22 GMT"
Server: "Microsoft-IIS/7.5"
请求头 (0.437 KB)
Host: "localhost"
User-Agent: "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0"
Accept: "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8"
Accept-Language: "zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3"
Accept-Encoding: "gzip, deflate"
Cookie: "ppp=qqq"
Connection: "keep-alive"
Upgrade-Insecure-Requests: "1"
If-Modified-Since: "Thu, 08 Dec 2016 11:08:22 GMT"
If-None-Match: ""d7c6e7634351d21:0""

Roundcube命令执行漏洞安全威胁通告

综述

2016年12月6日（当地时间），blog.ripstech.com网站发布了一条关于Roundcube远程命令执行漏洞的消息。在Roundcube1.2.2及其以前的版本中，deliver_message()函数在调用PHP内建函数mail()时的第5个参数可由用户控制且未经恰当过滤，mail()函数被调用后会使得PHP执行sendmail程序，而未经过滤的第5个参数允许对sendmail程序进行配置，从而使得sendmail程序将邮件流量保存在文件中，攻击者可以利用这个机制通过发送邮件将恶意PHP文件写入webroot目录。

相关链接地址如下：
https://blog.ripstech.com/2016/roundcube-command-execution-via-email/

漏洞危害

成功利用漏洞后，可以导致远程命令执行。

受影响的版本

- Roundcube version 1.1.x < 1.1.7
- Roundcube version 1.2.x < 1.2.3

不受影响的版本

- Roundcube version 1.1.x = 1.1.7
- Roundcube version 1.2.x = 1.2.3

什么是Roundcube?

Roundcube Webmail是一个基于浏览器，支持多国语言的IMAP客户端，操作界面看起像一个桌面应用程序。它提供一个e-mail客户端应该具备的所有功能包括MIME支持,地址薄,文件夹操作,信息搜索和拼写检查等。（引用自《百度百科》）

漏洞成因

该漏洞的成因是，函数deliver_message()在调用mail()函数时所传入的第5个参数未经恰当过滤，导致攻击者可以对sendmail程序进行配置从而保存邮件流量到文件中，进而使攻击者有机会将恶意PHP文件写入服务器的webroot目录中。触发漏洞的代码如下所示：

program/steps/mail/sendmail.inc

```
$from = rcube_utils::get_input_value('_from', rcube_utils::INPUT_POST, true, $message_charset);
⋮
$sent = $RCMAIL->deliver_message($MAIL_MIME, $from, $mailto,$smtp_error, $mailbody_file, $smtp_opts);
```

上述代码从POST参数中获取“_from”的值，并且将其作为第二个参数传入deliver_message()函数。

program/lib/Roundcube/rcube.php

```
public function deliver_message(&$message, $from, $mailto, &$error, &$body_file = null, $options = null) {
  ⋮
  if (filter_var(ini_get('safe_mode'), FILTER_VALIDATE_BOOLEAN))
    $sent = mail($to, $subject, $msg_body, $header_str);
  else
    $sent = mail($to, $subject, $msg_body, $header_str, "-f$from");
```

而上述代码会把未经恰当过滤的参数传入mail()函数。

过滤失败的原因如下：

```
else if ($from_string = rcmail_email_input_format($from)) {
  if (preg_match('/(\S+@\S+)/', $from_string, $m))
    $from = trim($m1, '<>');
  else
    $from = null;
}
```

虽然上述代码对用户控制的参数进行了正则表达式匹配，对用户输入采取了过滤措施；然而该过滤措施只在rcmail_email_input_format()函数返回TRUE时才会被执行。下面看一下rcmail_email_input_format()函数的具体实现：

program/steps/mail/sendmail.inc

```
function rcmail_email_input_format($mailto, $count=false, $check=true)
{
  global $RCMAIL, $EMAIL_FORMAT_ERROR, $RECIPIENT_COUNT;
  // simplified email regexp, supporting quoted local part
  $email_regexp = '(\S+|("[^"]+"))@\S+';
  ⋮
  // replace new lines and strip ending ', ', make address input more valid
  $mailto = trim(preg_replace($regexp, $replace, $mailto));
  $items  = rcube_utils::explode_quoted_string($delim, $mailto);
  $result = array();
  foreach ($items as $item) {
    $item = trim($item);
    // address in brackets without name (do nothing)
    if (preg_match('/^<'.$email_regexp.'>$/', $item)) {
      $item    = rcube_utils::idn_to_ascii(trim($item, '<>'));
      $result[] = $item;
    }
    ⋮
    else if (trim($item)) {
      continue;
    }
    ⋮
  }
  if ($count) {
    $RECIPIENT_COUNT += count($result);
  }
  return implode(', ', $result);
}
```

上述代码中的“if (preg_match('/^< '.$email_regexp. '>$/' , $item))”可以被攻击者有意构造的数据匹配失败，从而导致变量$result为空，这在if条件判断中相当于FALSE，从而导致前面提到的过滤被绕过，最终导致漏洞的发生。

规避方案

官方已经发布了针对该漏洞的版本更新，建议用户升级到不受影响的最新版本，下载页面如下：

https://roundcube.net/download/

ImageMagick压缩TIFF图片远程代码执行漏洞安全威胁通告

综述

2016年12月3日，talosintelligence.com网站发布了一条关于ImageMagick远程代码执行漏洞的消息，漏洞编号为CVE-2016-8707。ImageMagick在压缩TIFF图片时存在可利用的内存越界写入问题，在特别情况下该问题会造成远程代码执行。

相关链接地址如下：

http://www.talosintelligence.com/reports/TALOS-2016-0216/

漏洞危害

成功利用漏洞后，导致远程代码执行。

受影响的版本

- ImageMagick version < 7.0.3-9

不受影响的版本

- ImageMagick version = 7.0.3-9

规避方案

官方已经在新版本中修复了该漏洞，建议用户升级到不受影响的最新版本（7.0.3-9版本），下载页面如下：

http://www.imagemagick.org/script/binary-releases.php

什么是ImageMagick?

ImageMagick软件是用C语言编写的，可用来显示、转换以及编辑图形，支持超过200种图像文件格式，并且可以跨平台运行。

ImageMagick软件被许多编程语言所支持，包括Perl，C++，PHP，Python和Ruby等，并被部署在数以百万计的网站，博客，社交媒体平台和流行的内容管理系统(CMS)。

OpenSSH远程代码执行漏洞安全威胁通告

综述

2016年12月19日，OpenSSH官网发布了一个OpenSSH的版本更新，在新版本中修复了编号为CVE-2016-10009的漏洞。该漏洞允许攻击者在运行ssh-agent(该程序通常运行在客户端)的机器上加载一个恶意模块PKCS#11从而使攻击者有机会执行远程代码。

相关链接地址如下：

http://www.openssh.com/txt/release-7.4

漏洞危害

成功利用漏洞后，导致远程代码执行。

受影响的版本

- OpenSSH version < 7.4

不受影响的版本

- OpenSSH version = 7.4

规避方案

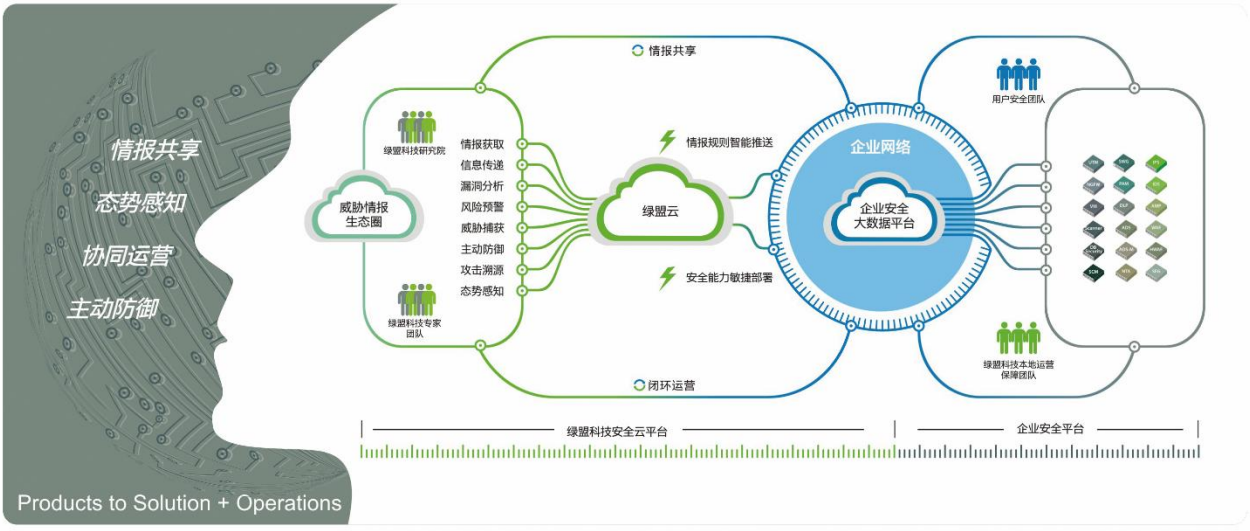
官方已经发布了该漏洞的版本更新，建议用户升级到不受影响的最新版本，下载页面如下：

http://www.openssh.com/portable.html

NSFOCUS

智慧安全2.0

智能·敏捷·可运营



关注绿盟科技官方微博

关注绿盟科技官方微信

www.nsfocus.com.cn

服务热线 400-818-6868

NSFOCUS

产品动态

NSFOCUS

产品动态

绿盟WEB应用防火墙系统（WAF）V6.0.6.0正式发布

绿盟 Web应用防火墙通过持续增强 Web 安全防护能力、丰富部署应用场景、优化设备自身安全运维能力，帮助客户保障 Web 业务安全并满足合规要求。新版本 V6.0R06F00（V6.0.6.0）于本月正式发布。

秘籍一 ：内家功法——吸星引擎

WAF6060集成了强大的吸星引擎，专门针对SQL注入和XSS攻击进行智能检测，从而提供更高的检测率和更低的误报率。同时，它与传统检测引擎并存，并基于站点特性提供友好的配置界面，用户可根据自身的实际需求进行个性化设置。作为一款新的检测引擎，WAF研发团队对其进行了长时间多方位的测试，除了强大的检测功能，更保证其对WAF的产品性能和稳定性无任何额外影响。

秘籍二 ：外家拳法——SSL加速

随着数据安全传输的需求日渐旺盛，基于HTTPS的站点也越来越多，而纯粹依靠软件的加解密技术已经不足以满足客户的实际性能需求。WAF6060新增的SSL加速功能，通过软硬件结合的方式，依靠SSL硬件加速卡解决了一直以来HTTPS协议解密存在的性能损耗问题，从而大大提升了WAF的HTTPS处理性能。同时，针对中高端WAF市场的高并发需求，产品团队应势推出了三款不同性能档位的E系列新型号——包括扩充CF卡，大幅增加内存，使得WAF产品可以提供更高的并发性能和更长的生命周期。

秘籍三：神助攻——IP信誉

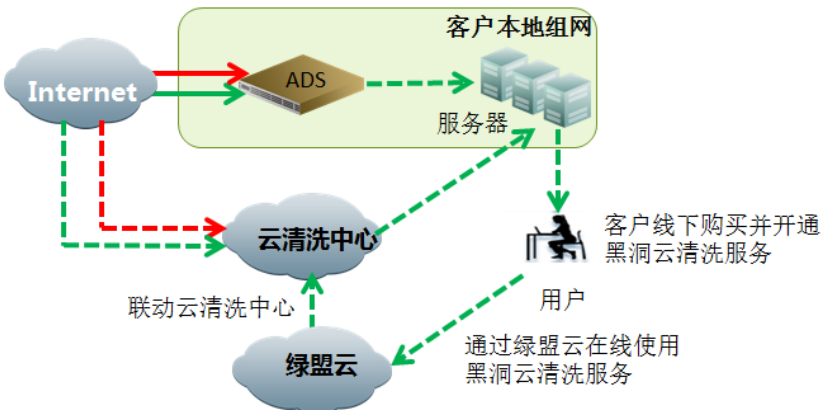
随着威胁情报的概念普及，单兵作战已经成为当前安全界的信息孤岛。WAF6060因势推出IP信誉功能，通过消费云端的海量IP信誉，达到情报实时共享、威胁实时阻截的目的。当前绿盟云端IP信誉已达到3100+万条，WAF会每日更新本地信誉缓存，使信誉消费的实时性和有效性达到最大发挥。

类别	功能	效果
安全防护	IP信誉	及时发现撞库、羊毛党行为
可维护性&可管理	支持设备策略配置迁移	满足双机切换、冷备设备配置同步、主备设备配置自动同步等运维场景需求。
合规	支持SNMP v3 web管理支持TLS v1.2	满足金融行业人行监管要求以及PCI DSS合规要求

DDOS攻击混合清洗方案

双十一、双十二、圣诞节、元旦、春节……。最近三个月的节日有点多，金融企业平台推出的客户优惠促销活动自然更多，由此带来的信息安全防护的工作压力相比之前，增加了不少，特别是防护攻击者针对这些互联网金融平台展开的DDOS攻击，俨然已经成为了这一阶段信息安全防护工作的重中之重。

面对突如其来的DDOS攻击，该如何应对呢？已经部署在网络出口的抗DDOS攻击设备要如何使用呢？如果攻击流量大，持续时间长，除了依靠安全设备以外还有其他更好的解决方法吗？下面就来介绍一下：DDOS攻击混合清洗解决方案。



如图所示，该方案由三个必要组件组成：

（1）、本地清洗设备ADS：绿盟抗DDOS攻击设备，部署在网络本地出口，对不超过带宽上限和设备性能上限的DDOS流量进行清洗；

（2）、云清洗中心：一旦攻击流量超出本地清洗设备的防护能力时，需要通过云清洗中心对大流量DDOS攻击进行防护，云清洗是一项专业清洗服务，购买后，攻击流量将被牵引到云清洗中心进行流量过滤，而服务器真实IP将作为被保护目标隐藏起来（如果攻击直接针对该IP，则建议关闭该IP，启用备用IP后，再根据情况进行流量牵引），过滤后得到的正常流量将放回目的地。

（3）、绿盟云：在绿盟云上，用户可以看到购买的云清洗服务的各项指标（如最大带宽值，服务剩余次数等），并且可以对防护目标进行策略配置（如域名、协议类型等）。

综上可知，第（1）和第（2）部分组成了DDOS攻击混合清洗方案的核心部分，其思路就是采用本地清洗+云清洗结合的方式对DDOS攻击进行防护，而第（3）部分主要是针对第（2）项服务所提供的用户操作和策略配置界面，且即便用户遭受的DDOS攻击超出了用户购买的云清洗服务的最大带宽，该项服务也将继续开启，自动为用户扩充带宽。

堡垒机SAS-H产品使用小技巧

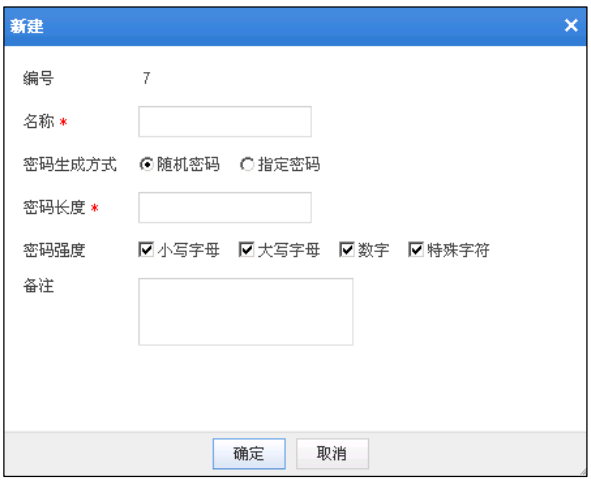
在金融行业，很多网络管理者需要使用“密码信封”功能，下面先解释一下什么是“密码信封”。

“密码信封”诞生的根源在于，管理者认为无论通过什么样的设备对运维人员进行运维规范管理，都无法阻止有人直接进入机房，在服务器本地进行恶意操作。这种对运维安全控制级别要求较高的企业最终认为，只有这些“恶意”的运维人员，在任意时刻都不知道目标系统的用户名和密码，才是真正安全的。

因此，定期对重要系统进行口令和密码重置，并且将修改后的口令采用安全的方式进行保存，然后所有运维人员均通过代理机进行运维跳转操作，便成为必然。而所有的口令和密码同时以纸质的方式，装在一个信封中，锁在保险柜里，这就是“密码信封”。不管企业里采用了什么密码保管的技术手段，一旦所有的安全策略全部失效这种小概率事件真的发生，则只有打开“密码信封”，才能进行运维操作。

“密码信封”会定期或不定期更新，并且由专人保管。

为了配合或逐渐取代“密码信封”这种需求，堡垒机产品中的自动改密功能就必不可少了，绿盟堡垒机中此类功能称为“密码对象”，密码对象分为密码规则和改密脚本。密码规则可以配置新密码的密码复杂度或为目标设备指定新密码，而改密脚本可以修改各类目标设备帐号的密码。



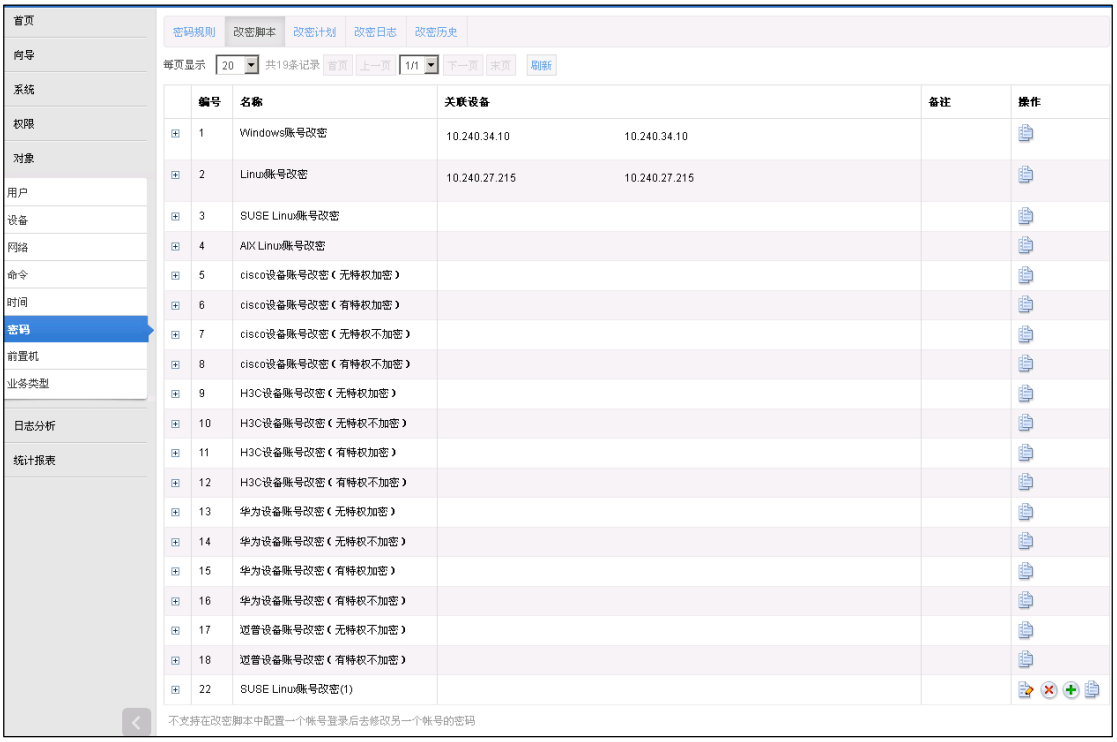
注意：只有设备管理员有配置密码对象的权限。

（1）密码规则：

如图所示，可对密码生成的规则进行设置：

（2）改密脚本：

如图所示，其中编号1～18是系统缺省的改密脚本，缺省的改密脚本不能编辑或删除，仅支持复制后作为新的改密脚本由设备管理员自定义修改。编号大于18的改密脚本是设备管理员自定义的改密脚本，支持编辑、复制、删除和添加操作：



不忘小配置，解决大问题。

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