国家互联网应急中心

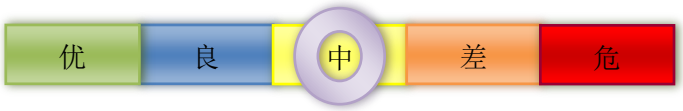
网络安全信息与动态周报

2016 年第 22 期

5 月 23 日-5 月 29 日

CNCERT/CC

本周网络安全基本态势

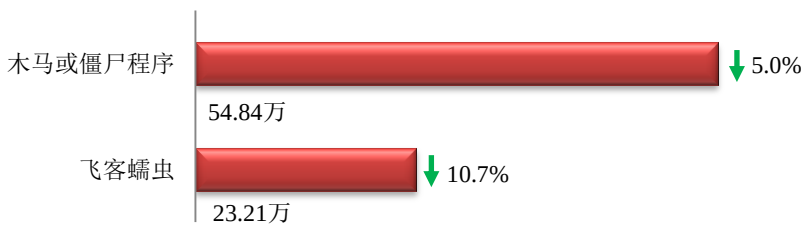


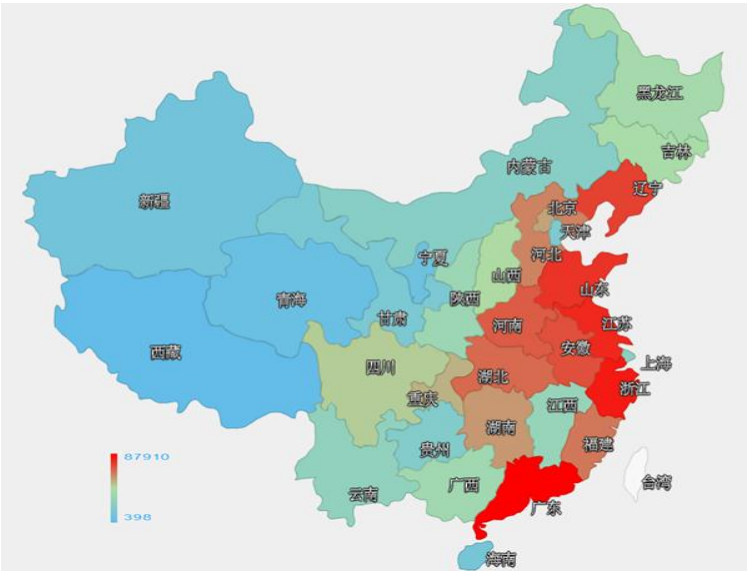
境内感染网络病毒的主机数量	• 78.05万	↓ 6.8%
境内被篡改网站总数 其中政府网站数量	• 2968 • 85	↓ 5.6% ↑ 11.8%
境内被植入后门网站总数 其中政府网站数量	• 3162 • 115	↓ 64.2% ↓ 50.0%
针对境内网站的仿冒页面数量	• 3225	↓ 33.7%
新增信息安全漏洞数量 其中高危漏洞数量	• 206 • 72	↓ 5.9% ↓ 13.3%

= 表示数量与上周相同　↑ 表示数量较上周环比增加　↓ 表示数量较上周环比减少

本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 78.05 万个，其中包括境内被木马或被僵尸程序控制的主机约 54.84 万以及境内感染飞客（conficker）蠕虫的主机约 23.21 万。



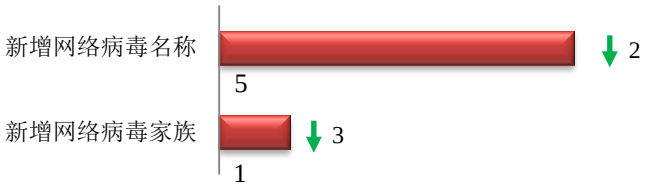


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、浙江省和江苏省。

TOP3

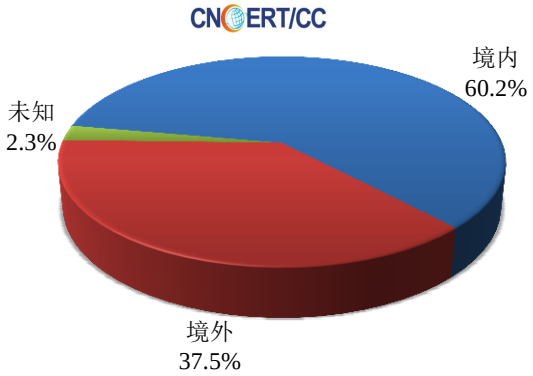
广东省	•约8.8万个（约占中国大陆总感染量的16.0%）
浙江省	•约7.7万个（约占中国大陆总感染量的14.0%）
江苏省	•约3.9万个（约占中国大陆总感染量的7.2%）

本周 CNCERT 捕获的新增网络病毒文件，按网络病毒名称统计新增 5 个，按网络病毒家族统计新增 1 个。

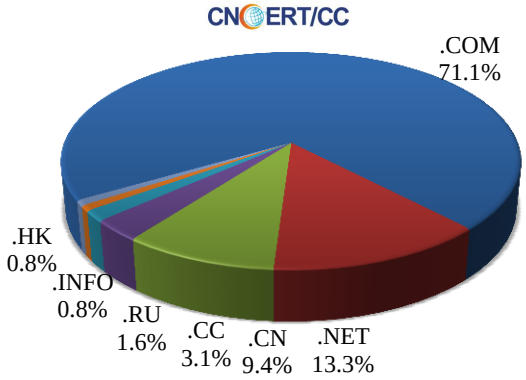


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 128 个，涉及 IP 地址 345 个。在 128 个域名中，有 37.5%为境外注册，且顶级域为.com 的约占 71.1%；在 345 个 IP 中，有约 8.7%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 25 个 IP。

本周放马站点域名注册所属境内外分布
(5/23-5/29)



本周放马站点域名所属顶级域的分布
(5/23-5/29)



针对 CNCERT 自主监测发现以及各单位报送数据，CNCERT 积极协调域名注册机构等进行处理，同时通过 ANVA 在其官方网站上发布恶意地址黑名单。

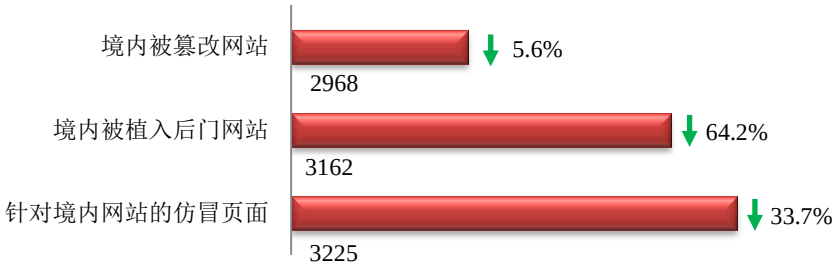
ANVA恶意地址黑名单发布地址

http://www.anva.org.cn/virusAddress/listBlack

中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由中国互联网协会网络与信息安全工作委员会发起、CNCERT 具体组织运作的行业联盟。

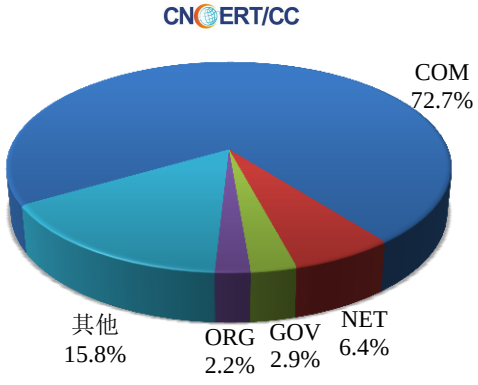
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2968 个；境内被植入后门的网站数量为 3162 个；针对境内网站的仿冒页面数量为 3225。

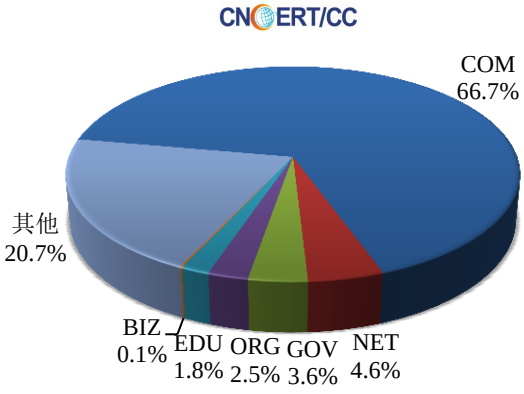


本周境内被篡改政府网站（GOV 类）数量为 85 个（约占境内 2.9%），较上周环比上升了 11.8%；境内被植入后门的政府网站（GOV 类）数量为 115 个（约占境内 3.6%），较上周环比下降了 50.0%；针对境内网站的仿冒页面涉及域名 1422 个，IP 地址 471 个，平均每个 IP 地址承载了约 7 个仿冒页面。

本周我国境内被篡改网站按类型分布
(5/23-5/29)

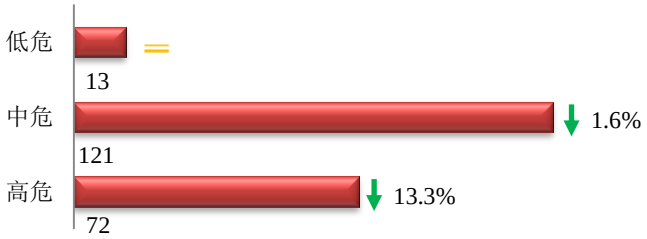


本周我国境内被植入后门网站按类型分布
(5/23-5/29)

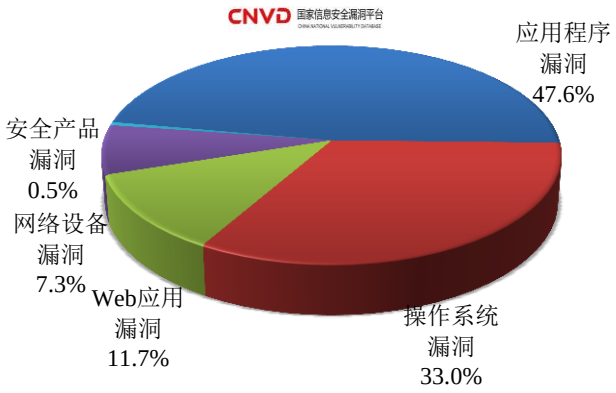


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 206 个，信息安全漏洞威胁整体评价级别为中。



本周CNVD收录漏洞按影响对象类型分布
(5/23-5/29)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是操作系统漏洞和 Web 应用漏洞。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

CNVD漏洞周报发布地址

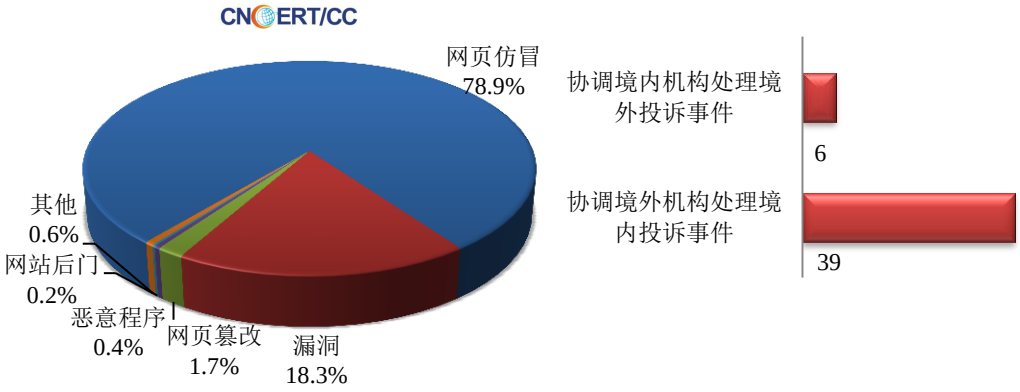
http://www.cnvd.org.cn/webinfo/list?type=4

国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

本周事件处理情况

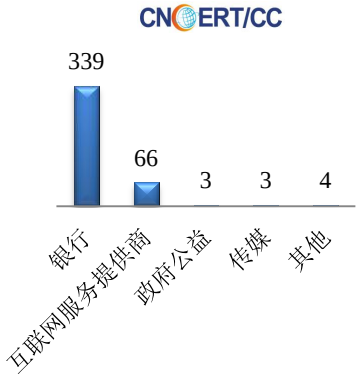
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 526 起，其中跨境网络安全事件 45 起。

本周CNCERT处理的事件数量按类型分布
(5/23-5/29)

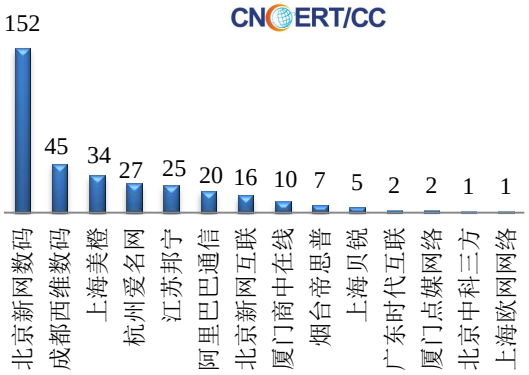


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 415 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事 339 起和互联网服务提供商仿冒事件 66 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(5/23-5/29)

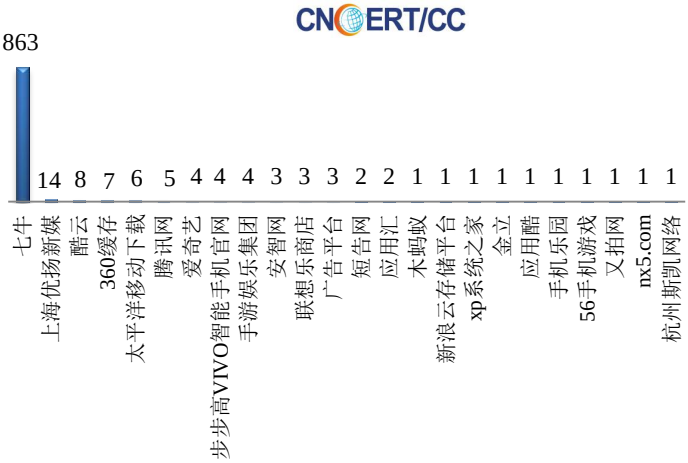


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (5/23-5/29)



本周，CNCERT 协调 24 个应用商店及挂载恶意程序的域名开展移动互联网恶意代码处理工作，共处理传播移动互联网恶意代码的恶意 URL 链接 938 个。

本周CNCERT协调手机应用商店处理移动互联网恶意代码事件数量排名 (5/23-5/29)



业界新闻速递

1、2016 中国网络安全年会在四川成都召开

CNCERT 网站 5 月 26 日消息 2016 年 5 月 25 日至 26 日，以“聚网络英才 • 筑安全生态”为主题的 2016 中国网络安全年会（第 13 届）在四川省成都市顺利召开，来自工业和信息化部、国防部、科技部、公安部、人社部、交通运输部、中国人民银行、四川省人民政府等单位的领导和专家，国内金融和电力等重要信息系统单位、基础电信企业、域名服务机构、互联网和网络安全企业、科研院所等业界同仁，以及来自 CNCERT 国际合作伙伴部分代表齐聚一堂。大会主办方国家互联网应急中心主任黄澄清致大会欢迎辞，对参会代表的到来表示了热烈的欢迎，对给予本次大会大力支持的各方表示衷心的感谢。工业和信息化部党组成员、办公厅主任莫玮出席会议并致辞，莫玮指出，我国互联网事业发展取得了显著成绩，突出体现在基础设施加快演进升级、产业规模持续扩大、融合创新蓬勃发展、国际影响力稳步提升四个方面。但与此同时，网络空间面临的威胁和挑战越来越现实和紧迫。莫玮就进一步做好网络安全工作提出四点要求：一是把握机遇，推动网络安全事业迈上新台阶；二是凝心聚力，加快突破网络安全核心技术；三是增进合作，不断提升网络安全保障能力；四是多措并举，持续壮大网络安全人才队伍。莫玮强调每个人都有责任积极发挥才干，投身网络强国建设，为共同推动我国互联网的持续健康发展贡献力量，希望参会代表在此次大会期间，多沟通交流，分享经验和思想，共谋网络强国建设大计。本次大会还同期举办了 2016 中国网络安全技术对抗赛，并开展了以“黑客入侵案例重现分析与业务保障对策”为主题的网络安全专场培训，分设了“网络安全威胁情报”、“网络安全人才培养”、“漏洞安全及价值秩序”、“移动互联网安全生态”、“数据安全分论坛”、“CNCERT-CIE 网络安全学术论坛”六个主题分论坛，为网络安全技术爱好者提供了交流、展示、学习网络安全技术的平台。大会由工业和信息化部指导，国家计算机网络应急技术处理协调中心（CNCERT）主办，中国电子学会、中国互联网协会网络与信息安全工作委员会和中国通信学会通信安全技术委员会协办。来自政府部门、重要信息系统、企业、行业协会、科研院所等单位以及 CNCERT 国际合作伙伴的代表共九百余人参加了本次大会。

2、美国海军准备为海军培训黑客技术

环球网 5 月 24 日消息 国外媒体报道称，美国海军已经为一个新的培训项目进行了招标，这个项目是旨在为海军们培训一些专门的黑客技术——美国海军称之为 ethical hacking 技术。这个培训项目的第一轮预计将在 6 月 6 日-10 日间进行，地点位于加州圣地亚哥，一个班 34 人。美国海军正在寻找经由美国电子商务顾问局（International Council of Electronic Commerce Consultants）或其授权合作伙伴认证过的讲师。政府的招标内容需求中有提到，海军技工需要被教授风险管理框架（Risk Management Framework）的 20 个关键安全控制（20 Critical Security Controls）。美国海军期望对海军进行基本的黑客技术培训，这可以用于理解外部的那些网络黑客是怎么想的。这些技能也可用于保护美国的关键设备和力量，在战场上也能抵御敌方在这方面的进攻。实际上按照 NextGov 的报道，美国陆军已经在进行类似的黑客项目培训，而且已经好几个月时间了。另外还有美国海军陆战队（US Marines，美军的一个下属部门）今年 3 月底宣布名为“Marine Corps Cyberspace Warfare Group”

队伍的成立，也是提供网络支持的。当前在美军之中，网络技能似乎存在越来越大的需求，美国空军去年年末也宣布在网络战争方面投入更多预算。

3、日本将成立网络防御政府机构保护关键基础设施安全

E 安全 5 月 23 日消息 日本《读卖新闻》报道称，日本正在考虑成立一个新的政府机构，专门抵御针对关键基础设施的网络攻击。这个新机构名为工业网络安全促进机构（ICPA），将于 2017 年正式投入运营。日本政府希望借此能够在 2020 年东京奥运会期间保护关键基础设施的安全。ICPA 的保护目标包括电力、天然气、石油、化学和核设施。此外，小型国防私营企业也将从中获益。从公布的情况来看，日本政府将组建的 ICPA 包含两个功能，一个是研究一个是主动响应。研发处将会跟本地大学和海外机构如美国国土安全局等开展联合研究和真实的网络演练。而主动响应处决定所采取的一切措施，它会对专家、白帽黑客进行入侵技术训练以阻止网络攻击并抗击已有的网络威胁。ICPA 的唯一目标是保护基础设施而且所有政府机构的安全。日本政府创建 ICPA 的原因是避免日本遭遇像乌克兰电网系统、美国电网和大坝系统近期遭 遇的网络攻击。这些关键系统不仅使用了电脑和移动设备还使用了关键 ICS/SCADA 系统，而现有的安全软件解决方案很少能够实施对后者的保护。如果 ICPA 成功组建，那么必须开发出专门针对工业系统的定制化安全解决方案。除了一些针对 SCADA 和普通 IT 网络之间空隙的安全协议之外，这些敏感的基础 设施并没有得到其它形式的保护。

4、韩空军官网遭黑客攻击连续 13 天无法正常使用

环球网 5 月 26 日消息 据环球网消息韩国《东亚日报》5 月 25 日报道称，韩国空军官网主页遭受黑客攻击，已经连续 13 天无法正常使用。韩国军方目前正在对恶意代码进行分析。韩国空军保守人士 24 日表示，官网主页 5 月初遭受黑客恶意攻击。空军本部立即对主页进行修复，修复失败后于 12 日向韩国国防部报告并切断了主页链接。韩国空军近日制作了临时主页，为防个人信息外流仅保留最基本的功能。目前，韩国空军临时主页上写有“服务器故障，将尽快修复”的文字。韩国军方透露，空军主页主要为现役军人使用，黑客欲通过恶意代码使军人电脑成为“僵尸电脑”，此后可传播恶意代码。由于韩国军方核心网络国防网直接与作战指挥等相连接，因此黑客可能是为进入国防网而攻击空军主页。

5、南非银行数据泄露 导致日本 1400 台 ATM 遭盗提 14.4 亿日元

E 安全 5 月 23 日消息 目前日本执法部门正在调查一起安全事故，据称某个拥有上百名攻击者的犯罪组织在本月 15 号从遍布日本全国的 1400 台便利店自动取款机（简称 ATM）处窃得 14.4 亿日元（折合 1300 万美元），而整个过程仅耗时两个半小时。根据《日本新闻》报道，某国际网络犯罪组织利用泄露自一家南非银行的数据伪造信用卡，目前国际刑警组织正配合执法部门进行调查。日本警方还计划利用安保摄像头帮助寻找犯罪嫌疑人。此次被设为目标的 ATM 设备安装在爱知县、福冈、神奈川县、大阪以及东京，该团队从总计 1400 台 ATM 机上各提取 10 万日元——考虑到 ATM 设备的每天提款上限为 10 万日元，那么全部入侵活动总计造成 14.4 亿日元巨额损失。有关部门透露称，在这两个多小时之内，日本各银行发现全国各地出现了超过 1600 次与该南非银行相关的信用卡使用活动。目前日本与南非政府当局都没有报告任何银行数据泄露详情，不过根据当前情况看其很可能是将事态隐瞒了下来。银行在面对数据泄露事故时，往往与其它网站或 Web 服务同样难以应对。然而一旦银行数据流出，欺诈分子能够快速利用其制作出伪造卡片，并借此在几天内轻松将相关账户内的资金

提取出来。

6、SWIFT 系统第三家银行曝遭网络劫匪抢走 1200 万美元

安全牛网 5 月 23 日消息 南美一家银行日前站出来承认遭到网络攻击，其 SWIFT 银行间支付系统安全性被破坏。厄瓜多尔南方银行（Banco del Austro）遭到与今年 2 月孟加拉央行 9.51 亿美元劫案类似的网络攻击，损失 1200 万美元。今年 4 月，越南先锋商业股份银行（TPBank）也被网络劫匪锁定，所幸攻击行动被挫败，没有遭到损失。然而，南方银行的攻击是在 15 个月之前，几乎比几个月前孟加拉央行的惊天网络劫案早了近 1 年。这意味着，采用针对性恶意软件攻击银行国际支付系统的活动，可能比原先估计的还要疯狂。该消息是从纽约一起诉讼案中传出的——南方银行状告代理国际银行转账的美国富国银行。而为银行间转账提供基础设施的支付组织 SWIFT，则单独敦促各家银行要在网络攻击信息共享上更迈进一步。5 月 20 日，SWIFT 在一份声明中写道：“我们特别提醒所有用户，请遵守自身职责，及时报告 SWIFT 任何可疑的利用本行 SWIFT 连接进行诈骗的行为。我们正努力加强客户访问 SWIFT 网络的安全性。”2016 年 2 月孟加拉央行网络劫案中，由于一个低级拼写错误导致其中一笔转账遭到代理银行质疑，攻击计划被半途腰斩，大约 2000 万美元被追回，但网络窃贼们依然卷走了 8100 万美元。

关于国家互联网应急中心（CNCERT）

国家互联网应急中心是国家计算机网络应急技术处理协调中心的简称（英文简称为 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，是一个非政府非盈利的网络安全技术协调组织，主要任务是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全、保障基础信息网络和网上重要信息系统的安全运行。目前，CNCERT 在我国大陆 31 个省、自治区、直辖市设有分中心。

同时，CNCERT 积极开展国际合作，是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 正式成员，也是 APCERT 的发起人之一，致力于构建跨境网络安全事件的快速响应和协调处置机制。截止 2015 年，CNCERT 与 66 个国家和地区的 165 个组织建立了“CNCERT 国际合作伙伴”关系。

联系我们

如果您对 CNCERT《网络安全信息与动态周报》有何意见或建议，欢迎与我们的编辑交流。

本期编辑：何世平

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158