国家互联网应急中心

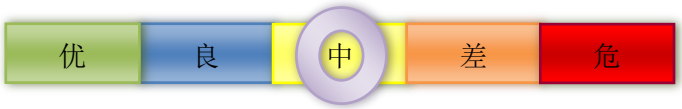
2015 年第 31 期

7 月 27 日-8 月 2 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

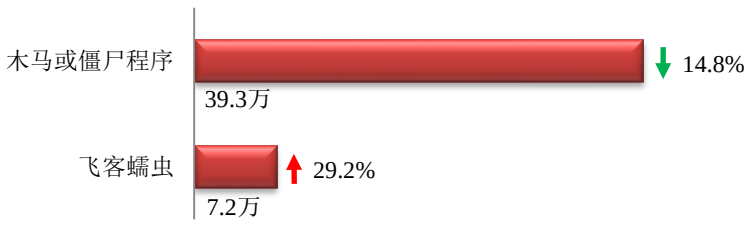


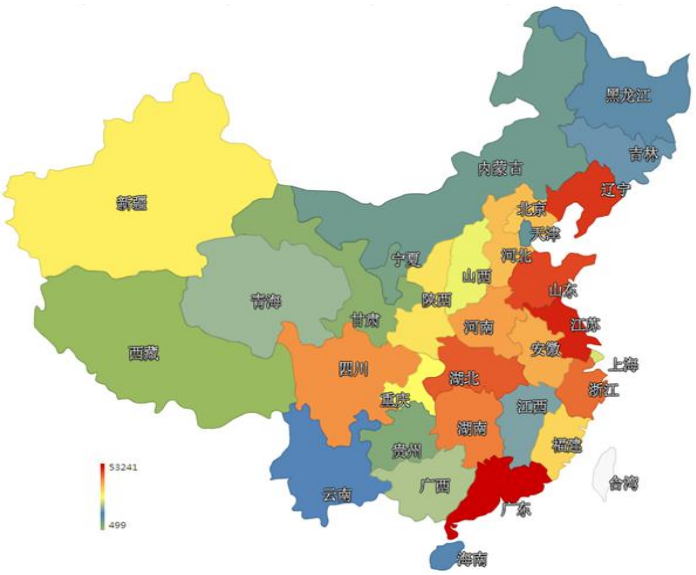
境内感染网络病毒的主机数量	•46.5万	↓ 10.1%
境内被篡改网站总数 其中政府网站数量	•5434 •118	↑ 104.9% ↑ 81.5%
境内被植入后门网站总数 其中政府网站数量	•4790 •144	↑ 65.6% ↑ 24.1%
针对境内网站的仿冒页面数量	•5399	↑ 9.8%
新增信息安全漏洞数量 其中高危漏洞数量	•228 •58	↑ 19.4% ↓ 24.7%

═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 46.5 万个，其中包括境内被木马或被僵尸程序控制的主机约 39.3 万以及境内感染飞客（conficker）蠕虫的主机约 7.2 万。



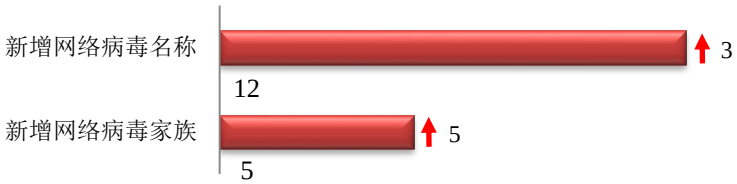


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、江苏省和辽宁省。

TOP3

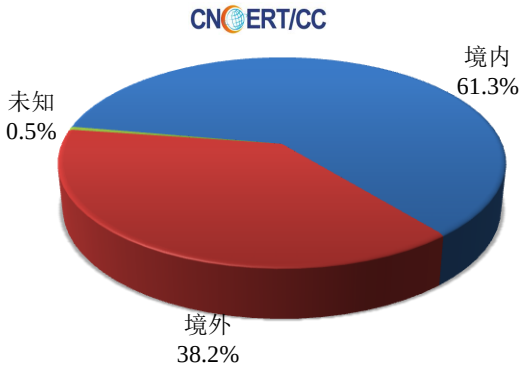
广东省	•约5.3万个（约占中国大陆总感染量的13.5%）
江苏省	•约4.1万个（约占中国大陆总感染量的10.3%）
辽宁省	•约3.2万个（约占中国大陆总感染量的8.2%）

本周 CNCERT 捕获了大量新增网络病毒文件，按网络病毒名称统计新增 12 个，按网络病毒家族统计新增 5 个。

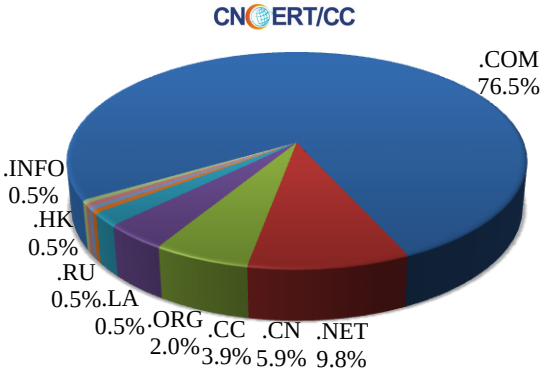


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 204 个，涉及 IP 地址 332 个。在 204 个域名中，有约 38.2%为境外注册，且顶级域为.com 的约 76.5%；在 332 个 IP 中，有约 13.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 48 个 IP。

本周放马站点域名注册所属境内外分布
(7/27-8/2)



本周放马站点域名所属顶级域的分布
(7/27-8/2)



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。

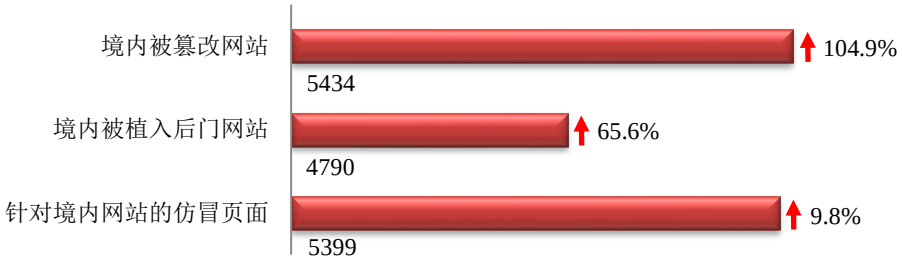
ANVA恶意地址黑名单发布地址

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。

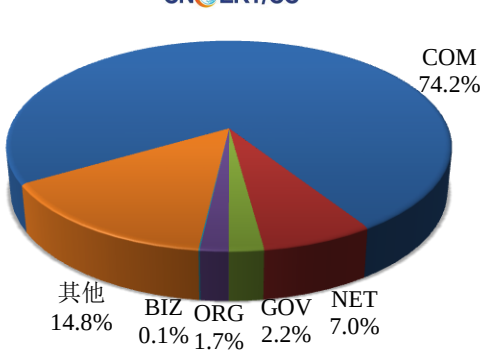
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 5434 个；境内被植入后门的网站数量为 4790 个；针对境内网站的仿冒页面数量为 5399。

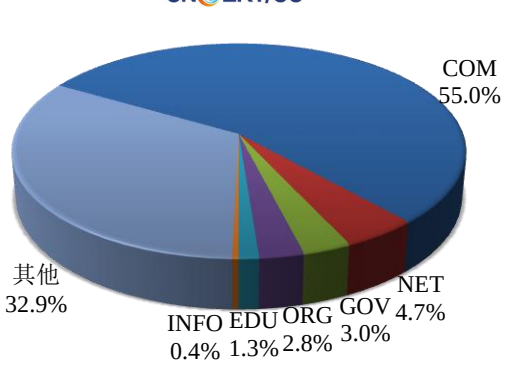


本周境内被篡改政府网站(GOV 类)数量为 118 个（约占境内 2.2%），较上周环比上升了 81.5%；境内被植入后门的政府网站(GOV 类)数量为 144 个（约占境内 3.0%），较上周环比上升了 24.1%；针对境内网站的仿冒页面涉及域名 4434 个，IP 地址 1032 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(7/27-8/2)

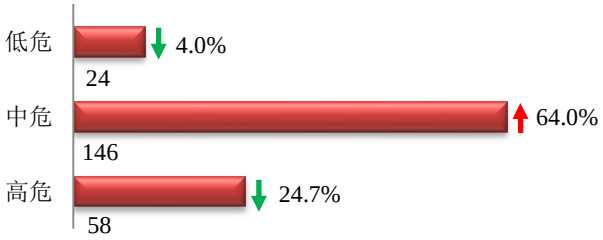


本周我国境内被植入后门网站按类型分布
(7/27-8/2)

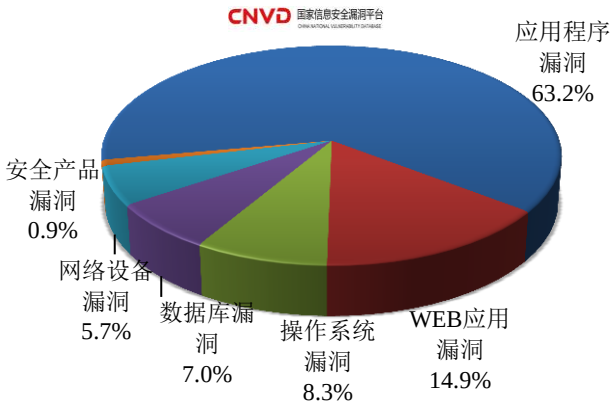


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 228 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
(7/27-8/2)



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 WEB 应用漏洞和操作系统漏洞。

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

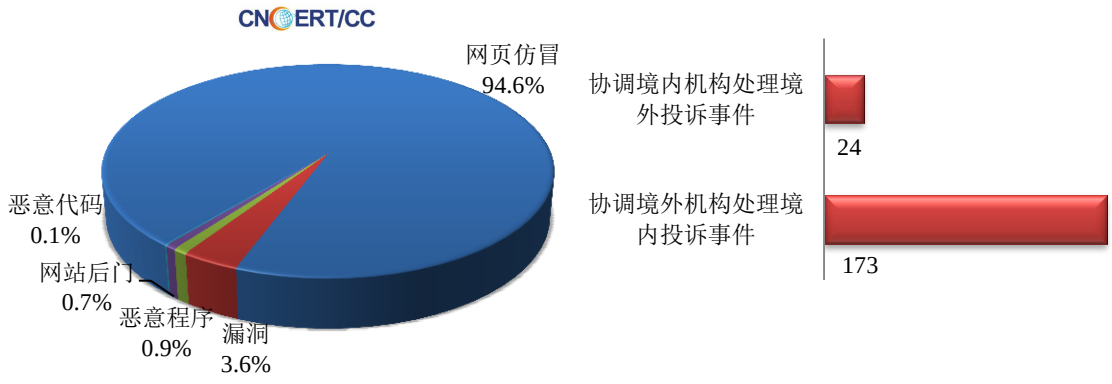
http://www.cnvd.org.cn/webinfo/list?type=4

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

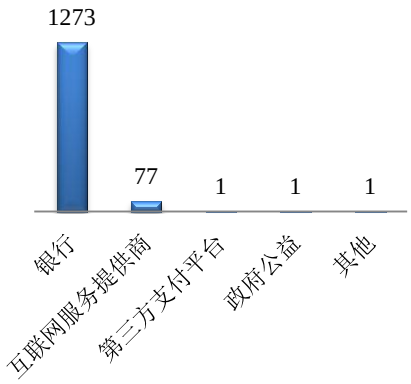
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 1430 起，其中跨境网络安全事件 197 起。

本周CNCERT处理的事件数量按类型分布
(7/27-8/2)

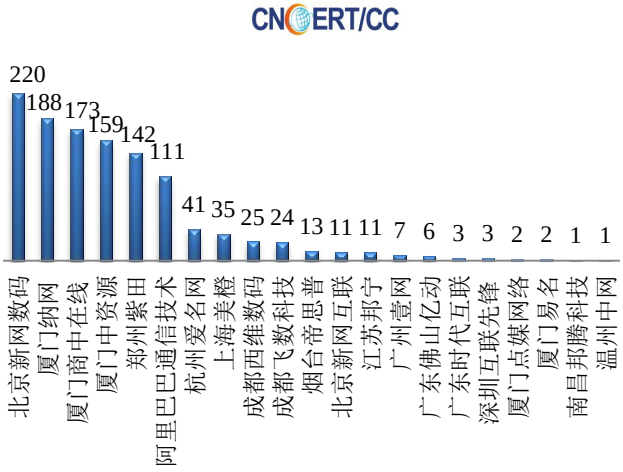


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1353 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 1273 起和互联网服务提供商仿冒事件 77 起。

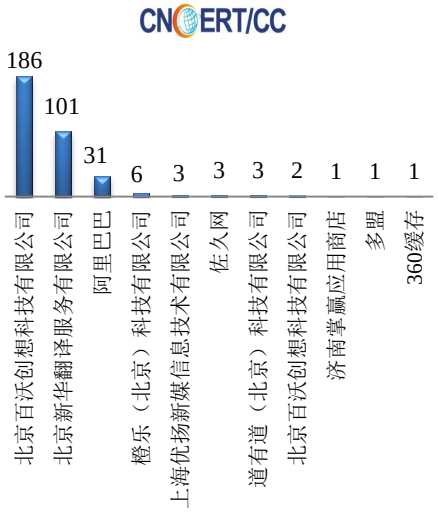
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (7/27-8/2)



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 (7/27-8/2)



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 (7/27-8/2)



本周，CNCERT 协调 11 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 338 个。

业界新闻速递

1、互联网网络安全威胁治理行动启动会在京召开

2015 年 7 月 31 日，国内 24 家单位在京举办互联网网络安全威胁治理行动启动会（以下简称“行动”），并在会上共同签署《互联网网络安全威胁治理行动承诺书》。国家互联网应急中心（CNCERT）和中国互联网协会网络与信息安全工作委员会主持召开启动会，并牵头组织开展此次行动。近年来，随着互联网技术的快速发展和应用，特别是移动互联网、云计算、大数据、物联网等新技术、新业务的风起云涌，人民群众日常工作、生

活对互联网的依赖程度越来越高。受经济利益驱动，以拒绝服务攻击（DDOS）、窃取公民个人信息、网页篡改、网络钓鱼、恶意程序、恶意移动应用程序（APP）等为代表的威胁互联网网络安全的行为呈快速增长趋势。威胁互联网网络安全的行为涉及多个环节，例如黑客需要连接互联网、注册域名、托管用于攻击的服务器、发布推广攻击工具和服务，涉及到了基础电信企业、域名注册服务商、数据中心（IDC）、搜索引擎和互联网企业等。因此，互联网网络安全威胁的治理需要多方的共同参与，发挥各自的技术和资源优势，规范各自的行为并承担相应的社会责任。本次行动将以行业自律的方式，动员行业内相关单位，从加强监测入手，通过密切配合、积极处置、曝光攻击者黑名单等措施，有效防范和治理威胁互联网网络安全的行为。同时，在行动开展期间，CNCERT 和中国互联网协会网络与信息安全工作委员会接收来自广大网民的互联网网络安全威胁举报，并积极开展核实处置工作。

2、NSA 监听数据将在 6 个月内全部销毁

新浪网 7 月 29 日消息 美国国家情报总监办公室（ODNI）周一宣布称，美国国家安全局（NSA）将限制数据读取并最终销毁曾经收集到的数以百万计的美国电话记录。上个月初，美参议院以 67 票赞成、34 票反对的结果通过了众议院之前通过的《美国自由法案》，根据《美国自由法案》，NSA 将在 6 个月的时间里逐步将大规模电话元数据收集项目转给电信公司，这也意味着这一政府大规模数据收集项目将宣告寿终正寝。由前中情局（CIA）职员爱德华·斯诺登曝光 NSA 自 2007 年小布什时期起开始实施的绝密电子监听计划，已过去两年，这期间斯诺登陆续曝出新的消息，主要为 NSA 监控美国公民的电子邮件、聊天记录、视频及照片等秘密资料。法国国外安全总局前局长阿兰·舒埃后来表示，在情报圈里，NSA 的监听计划从来都是公开的秘密，所有人都知道，NSA 自 2003 年起就开发了一个从全球获取数据的系统。尽管《美国自由法案》已得到美国众议院的法案通过，但在这 6 个月的“宽限期”中，自由法案还不能有效禁止 NSA 搜集数据。而且据报道称，美国政府正试图利用自由法案的部分条款，来暂时重启该项目。申请重启的理由是，将国内监控的工作“过渡”到电话公司身上。根据《自由法案》，今后将由电信公司来负责收集和存储这些数据，国安局只在确认某人或某个组织有恐怖活动嫌疑的时候才能向电信公司索取相关数据。

3、美媒：五角大楼开发网络武器称防止网络攻击

网易 8 月 2 日消息 美国在承受了一次又一次网络攻击后终于忍不住了。近日来自《洛杉矶时报》的消息显示，美五角大楼决定是时候展现真正的技术了。这个给世界带来第一朵蘑菇云的国家又在计划一项野心勃勃的工程：制作一种足够强大的网络武器，它一击就可以让他国政府失去攻击美国数据库和关键电脑系统的能力。很明显，比起永远不用发射的武器，五角大楼更相信只需要发射一次的武器。美国防部的意图在于把冷战时期阻止世界性核武战争的理念复制到 21 世纪电子战场。科技发展到今天，“网络威慑”计划无非是想把这一状况复制到数字时代。美国国家安全官员最近加强了设计这种武器的呼声。但尽管遭受的攻击次数日益增长，奥巴马政府还没有就应对手段达成一致。设计一种用于回击的网络武器在某些方面比回击核武打击更复杂。其中一个问题就是网络武器可能产生“误伤”。智囊团曾警告白宫如果美国决定开发以牙还牙的网络攻击手段，其造成的后果很可能是毁掉整个万维网系统。尽管互联网由美国电子工程师发明，但目前美国的电脑系统却不能抵挡接连不断的黑客攻击。另一个困难在于确认攻击者。如果一颗核弹头被射向美国本土，确定它的来源并不复杂，但网络攻击则不然。尽管如此，美军方官员相信在足够的时间里，他们可以研发出能够满足上述要求的武器。

4、韩国情院曾进行 200 多次黑客攻击多数行动失败

中新网 7 月 29 日消息 据韩媒报道，韩国政界一位有关人士表示，韩国国情院利用黑客软件，试图进行黑客攻击行动的次数多达 200 多次。据报道，该人士表示，韩国国情院共 200 多次以入侵电脑或手机的方式进行黑客攻击行动，但由于攻击目标未打开电子邮件上的附件，大多数黑客攻击行动均宣告失败。报道称，韩国国情院通常利用电子邮件发送黑客软件，如收件人两个月内没有打开这一电子邮件上附加的软件，就会被自动删除。另外，韩国新国家党议员李喆雨 29 日表示，本月 18 日自尽的国情院工作人员林某就是购买黑客软件和进行黑客攻击行动的负责人，他在遗书中谈到了近期引发争议的国情院黑客攻击案的相关内容。林某手下还有 4 个研究员，他们对林某进行黑客攻击实验工作给予了技术上的支援。此后，在野党向检方举报，要求检方对国情院利用黑客攻击软件入侵国内人士手机或个人用电脑的疑惑进行调查。韩国国情院院长李炳浩 27 日在国会情报委员会会议上说，最近自尽的国情院工作人员删除的网上文件是实验用文件，并非是为窃听或监视国内人士而研发的文件。李炳浩强调说，从过去至今，国情院从未对国内人士进行窃听或行踪追查。这番话如不属实，他将立刻辞去国情院院长一职。

5、厄瓜多尔政府采取措施加强网络安全防范

新浪网 7 月 28 日消息 厄瓜多尔《商报》7 月 27 日报道，自 2010 年以来，厄瓜多尔政府和企业网站已经遭受 100 次以上黑客袭击，其中不乏厄国会、财政部、环保部、交通和公共工程部等重要部门，因资料泄露、系统维护所造成的损失较大。美洲国家组织在其关于网络安全的最新报道中，称厄瓜多尔并没有准备好应对可能的网络攻击，且用于维护网络安全的相关预算很低。为了改变这种局面，厄政府开始重视网络安全。厄瓜多尔特别划拨 800 万美元预算，计划在军方成立网络指挥部，建立反网络攻击系统，并开始对人员进行技术培训。同时厄政府将加强国家情报系统的人员设施配置，希通过增强抵御性措施，保护政府网站系统的健康运行。

6、安卓曝致命漏洞黑客发彩信便可控制手机

新华网 7 月 29 日消息 网络安全公司 Zimperium 研究人员 7 月 27 日警告，全球应用最广泛的移动设备操作系统之一安卓（Android）存在“致命”安全漏洞，“黑客”只需简单发送一封彩信便能在用户毫不知情的情况下完全控制手机。Zimperium 当天在博客发帖说，公司研究人员乔舒亚·德雷克在安卓平台的核心组成部分，即主要用来处理、播放和记录多媒体文件的 Stagefright 框架中发现多处安全漏洞。“黑客”只需知道用户手机号码，便可通过发送彩信的方式远程执行恶意代码。具体而言，用户接收彩信后通过浏览器下载一个特制媒体文件，“黑客”就可以发动攻击。最可怕的是，Stagefright 框架不只能用来播放媒体文件，还能自动产生缩略图或从视频或音频文件中抽取元数据，这意味着“黑客”可以在用户完全不打开或阅读彩信的情况下入侵手机，甚至赶在用户看到这条彩信前将其删除，神不知鬼不觉地“黑”掉手机，继而远程窃取文件、查收电邮乃至盗取用户名和密码等信息，而用户对这一切全然不知。“这类攻击的目标可以是任何人，”Zimperium 公司说，“这些漏洞极其危险，因为它们无需受害人采取任何行动。”按这家公司的说法，Stagefright 框架的安全漏洞波及安卓多个版本，由于更新较慢，预计当前约有 95%、即多达 9.5 亿部使用安卓系统的智能手机受到影响。这家公司先前已将这些安全漏洞通报给谷歌公司，同时向后者提供了自行开发的补丁程序。“谷歌行动及时，48 小时内便在内部代码库应用了补丁程序，”Zimperium 公司说，“不过，这只是个开始，更新部署将是非常漫长的过程。”目前，谷歌已把补丁程序提供给合作伙伴，但补丁到达终端用户手中往往需要几个月时间。Zimperium 公司说，他们将于下月初在美国拉斯韦加斯举行的全球信息安全领域顶尖峰会“黑帽大会”上发布更多相关信息。

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 2014 年，CNCERT 与 63 个国家和地区的 144 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：徐娜

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990170