国家互联网应急中心

网络安全信息与动态周报

2016 年第 34 期

8 月 15 日-8 月 21 日

CNCERT/CC

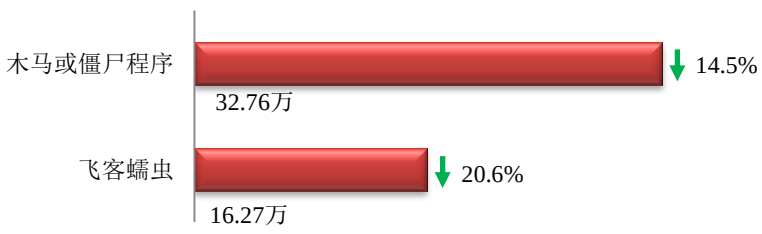
本周网络安全基本态势

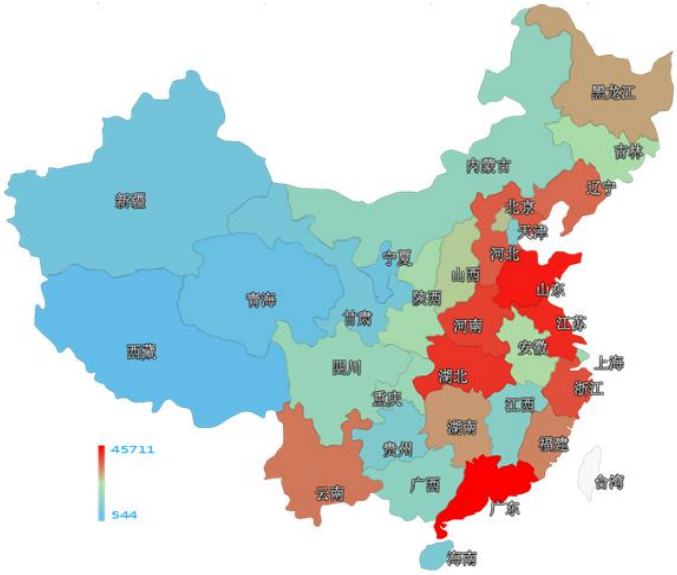
境内感染网络病毒的主机数量	•49.03万	16.6%
境内被篡改网站总数 其中政府网站数量	•4074 •90	0.8% 11.1%
境内被植入后门网站总数 其中政府网站数量	•2330 •90	10.5% 9.8%
针对境内网站的仿冒页面数量	•9384	14.3%
新增信息安全漏洞数量 其中高危漏洞数量	•189 •81	13.7% 3.8%

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 49.03 万个，其中包括境内被木马或被僵尸程序控制的主机约 32.76 万以及境内感染飞客（conficker）蠕虫的主机约 16.27 万。





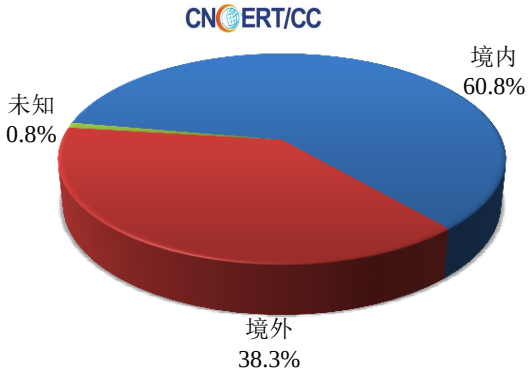
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、山东省和江苏省。

TOP3

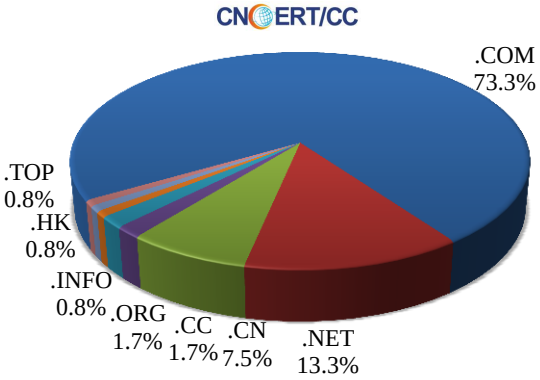
广东省	•约4.6万个（约占中国大陆总感染量的14.0%）
山东省	•约4.1万个（约占中国大陆总感染量的12.5%）
江苏省	•约2.2万个（约占中国大陆总感染量的6.6%）

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 120 个，涉及 IP 地址 327 个。在 120 个域名中，有 38.3%为境外注册，且顶级域为.com 的约占 73.3%；在 327 个 IP 中，有约 5.2%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 12 个 IP。

本周放马站点域名注册所属境内外分布
(8/15-8/21)



本周放马站点域名所属顶级域的分布
(8/15-8/21)



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。

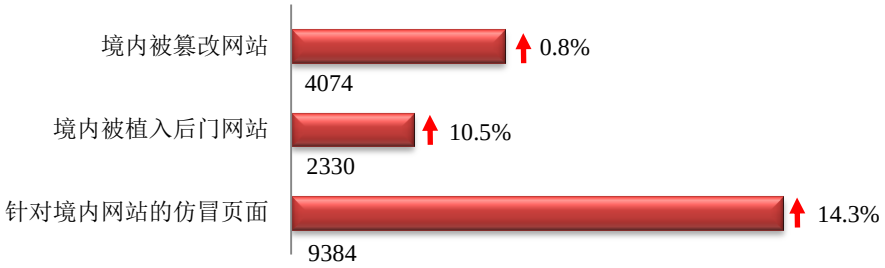
ANVA恶意地址黑名单发布地址

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。

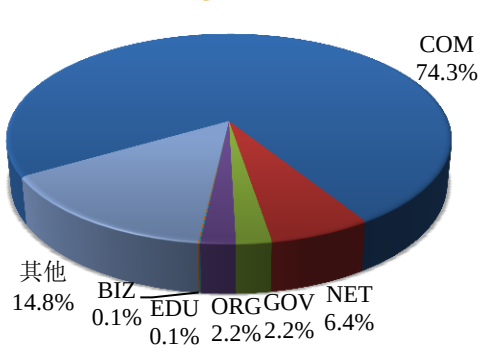
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 4074 个；境内被植入后门的网站数量为 2330 个；针对境内网站的仿冒页面数量为 9384。

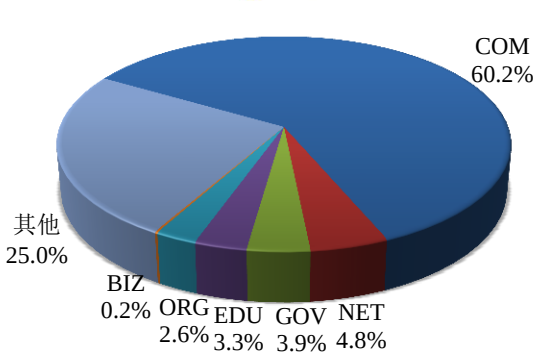


本周境内被篡改政府网站（GOV 类）数量为 90 个（约占境内 2.2%），较上周环比上升了 11.1%；境内被植入后门的政府网站（GOV 类）数量为 90 个（约占境内 3.9%），较上周环比上升了 9.8%；针对境内网站的仿冒页面涉及域名 1709 个，IP 地址 570 个，平均每个 IP 地址承载了约 16 个仿冒页面。

本周我国境内被篡改网站按类型分布
(8/15-8/21)

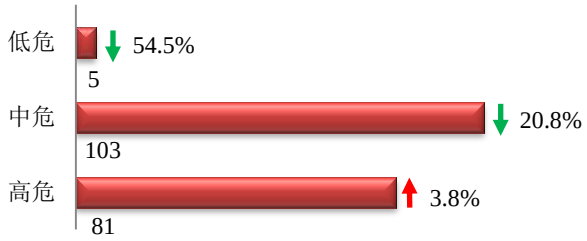


本周我国境内被植入后门网站按类型分布
(8/15-8/21)

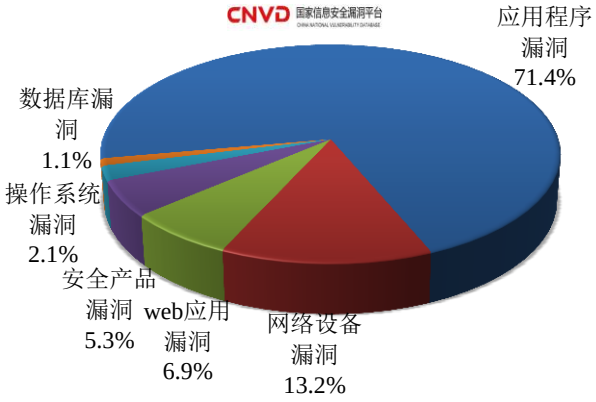


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 189 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
(8/15-8/21)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是网络设备漏洞和 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

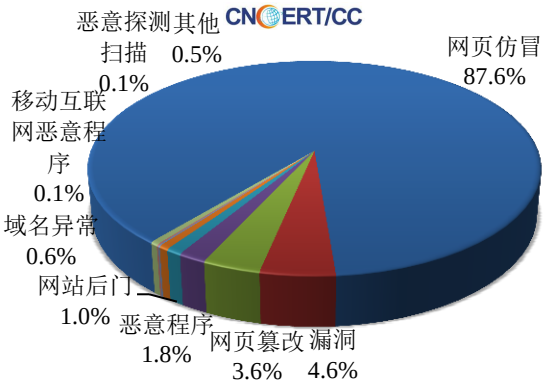
http://www.cnvd.org.cn/webinfo/list?type=4

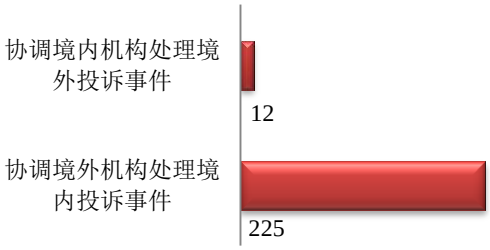
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 798 起，其中跨境网络安全事件 237 起。

本周CNCERT处理的事件数量按类型分布
(8/15-8/21)

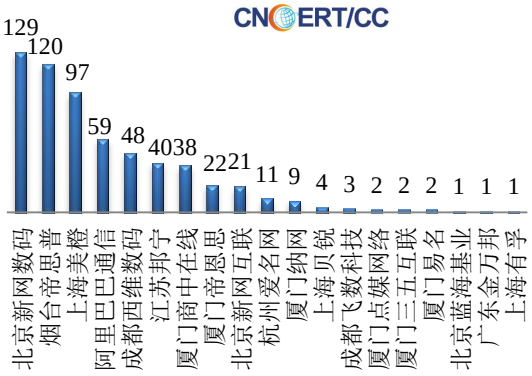




本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 697 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事 657 起和互联网服务提供商仿冒事件 34 起。

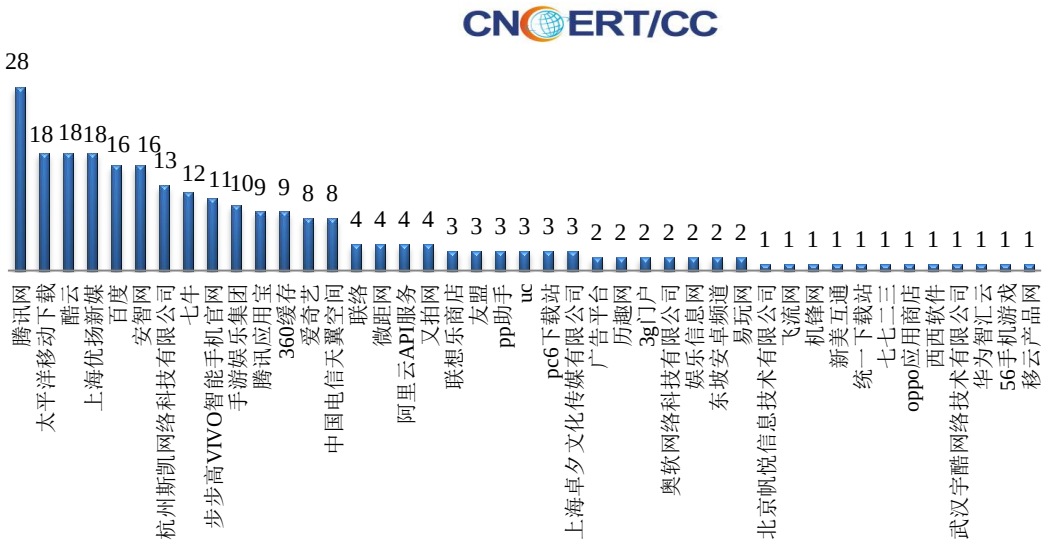
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(8/15-8/21)

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 (8/15-8/21)



本周，CNCERT 协调 43 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 254 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 (8/15-8/21)



业界新闻速递

1、2016 中国互联网安全大会在京举行

工信部网站 8 月 19 日消息 2016 年 8 月 16 日，在中央网信办网络安全协调局、工业和信息化部网络安全管理局、公安部网络安全保卫局联合指导下，以“协同联动，共建安全命运共同体”为主题的第四届中国互联网安全大会在北京召开。工业和信息化部网络安全管理局局长赵志国出席大会并致辞。会上，赵志国围绕落实责任、提升能力、完善机制，对企业做好网络安全工作提出三方面工作希望。一是落实四项安全责任，即落实企业内部的网络安全组织领导和管理责任、网络基础设施安全防护责任、保障数据和用户个人信息安全责任以及维护健康有序互联网环境责任。二是提升四种安全能力，即提升常态深入的威胁隐患排查能力、主动灵活的威胁发现能力、迅速高效的应急处置能力和准确可回溯的攻击溯源能力。三是完善四个合作机制，即构建“产、学、研、用”共同参与的技术交流合作机制，构建多方参与、规范有序的网络威胁信息共享机制，完善稳定、顺畅的网络安全应急协作机制，以及强化灵活、平等的网络安全行业自律机制。本次大会由中国互联网协会、中国网络空间安全协会和 360 互联网安全中心共同主办，来自全球 70 多家相关机构和企业的代表发表演讲，共同探讨网络安全话题，3 万余名网络安全行业人士围绕世界网络安全形势、网络空间战略、网络安全攻防实战、网络空间国际合作、产业方向及趋势、技术发展和人才培养等方面展开讨论。

2、“墨子号”开启星际首航 探索永久解决信息安全问题

光明网 8 月 19 日消息 被命名为“墨子号”的中国首颗量子科学实验卫星 8 月 16 日晨开启星际之旅。它承载着率先探索星地量子通信可能性的使命，并将首次在空间尺度验证量子理论的真实性。在量子卫星首席科学

家潘建伟院士看来，如果说地面量子通信构建了一张连接每个城市、每个信息传输点的“网”，那么量子科学实验卫星就像一杆将这张网射向太空的“标枪”。当这张纵横寰宇的量子通信“天地网”织就，海量信息将在其中来去如影，并且“无条件”安全。“传统的信息安全都是依赖于复杂的算法，只要计算能力足够强大，再复杂的保密算法都能够被破解。量子通信能做到绝对安全，是由量子自身的特性所决定的，计算能力再强也破解不了，因此它是革命性的，可从根本上、永久性解决信息安全问题。”潘建伟说。量子通信系统的问世，点燃了建造“绝对安全”通信系统的希望。当前，量子通信的实用化和产业化已经成为各个大国争相追逐的目标。“在城市范围内，通过光纤构建城域量子通信网络是最佳方案。但要实现远距离甚至全球量子通信，仅依靠光纤量子通信技术是远远不够的。”潘建伟说。他解释说，因为量子的信息携带者光子在光纤里传播一百公里之后大约只有 1‰的信号可以到达最后的接收站，所以光纤量子通信达到百公里量级就很难再突破。但光子穿透整个大气层后却可以保留 80%左右，再利用卫星的中转，就可以实现地面上相距数千公里甚至覆盖全球的广域量子保密通信。

3、台湾宣布组建网军：2019 年底实现全面作战能力

中华网 8 月 15 日消息 台湾新任“国防部长”冯世宽近期确认了新政府有意组建台湾武装部队的第四个军种单位：“网军”（CyberArmy）。民进党早前发布的《国防政策蓝皮书》特别强调“整合当前军事单位与信息、通信、电子技术能力，从而在陆、海、空军种组成武装部队的结构上组建独立的第四军种部队”，台湾“国防部”在此之后正式宣布了这项决定。展望未来，台湾新成立的“网军”将在当前网络安全和网络战架构上增强其相关能力。据信，全新的网络军队将直接合并信息和电子战司令部以及其他“国防部”下属与信号或者电子情报行动和管理相关的机构，例如台军总参谋部的通信、情报和信息办公室。据报道，新组建的网络军队将达到 6000 人左右的规模，并且最快可在 2019 年底实现全面作战能力。台军还正式宣布，新组建网络军队的任务重点不再仅局限于保卫其内部网络，民事互联网也全部处于其任务范围。正如世界上许多其他国家和地区的军队一样，台湾军队依靠由于明显的安全考虑而与民事互联网进行物理隔绝的内部网络。台湾军事基地和设施使用的许多计算机和网络设备都可能被要求只接受遵守军事网络协议的访问请求。正因如此，新成立的网络军队可能会被划分为两种不同的类型，分别负责互联网安全（民事）和内部网络安全（军事）。

4、欧盟欲加强对互联网通讯服务的监管 限制其加密措施

凤凰网 8 月 16 日消息 北京时间 8 月 16 日消息，据外媒报道，近些年来，基于互联网的通信应用（如微软的 Skype 和 Facebook 的 WhatsApp）正在逐步取代传统的语音和短信服务。不过这场战斗显得有些不公平，因为运营商们需要遵守关于信息安全和保密的监管规定，而互联网巨头们则一身轻松。不过这一情况马上就要改变了，欧盟准备将监管范围扩大到这些应用，限制它们的加密方式。《金融时报》援引欧盟内部的一份文件显示，下个月欧盟委员会会将这些规定的适用范围拓展至提供互联网语音和消息服务的公司。这就意味着，在新的法规框架下，这些网络服务商就无法随意处理手上握有的用户通讯数据了。未来，它们甚至还要为政府提供紧急服务的接入号码。据悉，欧盟委员会将于今年晚些时候提出对电子隐私规定的修订，而欧盟电信业监管规定更广泛的修订将于今年 9 月启动，新的法规将替代 2002 年的“电子隐私法令”。在“电子隐私法令”的框架下，电信运营商必须保护用户的通信，确保网络安全，不得保留用户的位置和流量数据。欧盟的规定还允许各国政府出于国家安全和司法目的去限制保密权。而基于互联网的通信服务是全球运营商，它们可以将所收集的流量

数据和位置数据用于商业目的。

5、NSA 被黑 或有可能成为第二起 TheHackingTeam 事件

E 安全 8 月 16 日消息 根据国外媒体的最新消息，美国国家安全局（NSA）貌似遭到了黑客的攻击。这个黑客团伙声称他们入侵了 Equation Group（方程式组织），并将他们从该黑客组织的计算机系统中所获取到的大部分黑客工具全部泄漏在了互联网上。这一黑客团伙自称为 The Shadow Brokers（影子经纪人），目前他们已经开始在网上逐步公开盗窃所得的数据了。除此之外，该黑客团伙还表示，他们手中目前仍掌握着大量的机密数据，他们计划在网上举行一次拍卖会，并将这些机密信息出售给竞价最高的竞标者。就在两天以前，The Shadow Brokers 黑客组织已经将部分泄漏文件公布在了例如 Github 和 Tumblr 等网络平台上，但是这些文件目前已经被删除了。值得注意的是，在这些文件中还包括有 NSA 用于大规模监控活动的黑客工具在内。该黑客组织表示，如果他们收到了一百万个比特币（总价值大约为五亿六千八百万美金），那么他们就会将所有的泄漏文件全部发布出来。据了解，这伙黑客目前只提供了百分之六十的泄漏数据，剩下百分之四十的数据将会提供给拍卖竞价最高的人。该黑客组织表示，这些文件中包含有非常复杂的黑客工具，NSA 此前曾使用过这些来进行间谍活动。除此之外，在泄漏的文件中不仅包含有 C&C 服务器的安装脚本和配置文件，而且还有一些针对美国路由器和防火墙等网络设备制造商（例如 Cisco，Juniper 和 Fortinet）的黑客工具。

6、斯诺登证实美国网络攻击目标包括中国公司

新华社 8 月 21 日消息 美国“截击”网站 8 月 19 日证实，根据“棱镜”监听项目曝光者、美国前防务承包商雇员爱德华·斯诺登提供的最新文件，美国国家安全局网络“武器库”近日遭黑客组织侵入，业已泄露的文件显示，美国网络攻击目标中包括中国公司。“截击”网站由率先曝光斯诺登事件的前英国《卫报》记者格伦·格林沃尔德创建，旨在以新闻报道形式公开斯诺登曝光的文件。8 月 13 日，黑客组织“影子中间人”通过社交平台宣称攻入美国国家安全局网络“武器库”——“方程式组织”并泄露其中部分黑客工具和数据。根据斯诺登提供的文件，可以确认这些工具是美国国家安全局软件，其中部分软件属于秘密攻击全球计算机的强悍黑客工具。部分泄露文件显示，这些黑客工具针对的目标包括思科、瞻博网络、飞塔等公司路由器和防火墙产品，中国信息安全公司天融信也在黑客工具攻击目标之列。斯诺登提供的文件还显示，美国国家安全局在巴基斯坦、黎巴嫩的行动中使用过目前已被泄露的一些“网络武器”。俄罗斯网络安全厂商卡巴斯基去年发布监测报告说，“方程式组织”开发机构已经活跃近 20 年，是全球技术“最牛”的黑客组织之一。而据媒体报道，“方程式组织”与美国国家安全局关系密切，是一个该局可能“不愿承认的”部门，这在黑客圈几乎是尽人皆知的秘密。

7、食尸鬼行动攻击 30 多个国家超过 130 家企业 包括中国

E 安全 8 月 18 日消息 自 2015 年 3 月以来，一个组织严密的网络犯罪团伙对超过 30 个国家逾 130 家企业开展工业间谍活动。该组织主要将目标局限在活跃于工业领域的企业，比如石油化工、海军、军事、航空航天等行业。但不具体针对一个国家，攻击范围遍布全球：包括西班牙、巴基斯坦、阿联酋、印度、埃及、中国等。网络安全厂商卡巴斯基实验室表示，他们将该行动称之为食尸鬼行动 （Operation Ghoul），行动集中在 2016 年 6 月，6 月 8 日-6 月 27 最为活跃。在 2016 年 6 月，研究人员发现了大量鱼叉式网络钓鱼电子邮件中包含恶意附件。附件中的恶意软件基于在暗网公开售卖的鹰眼商业间谍软件，为攻击者提供大量黑客工具。一旦安装，

它会收集受害者 PC 的数据。包括：击键、剪贴板数据、FTP 服务器凭证、浏览器的账户数据、已安装应用程序信息等。攻击者在 EXE 文件中打包他们的 RAT，放在 ZIP 文件内通过鱼叉式钓鱼邮件发送给目标企业的高管。他们的主要动机是通过售卖窃取得来的知识产权、商业情报或受害者的银行账户赚取经济利益。这类组织可能会对任何企业实施攻击。虽然他们使用较简单的恶意工具，但攻击十分有效。

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：张腾

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158