国家互联网应急中心

2015 年第 43 期

10 月 19 日-10 月 25 日

网络安全信息与动态周报

CNCERT/CC

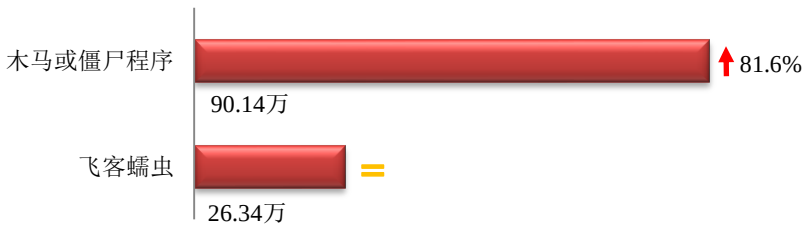
本周网络安全基本态势

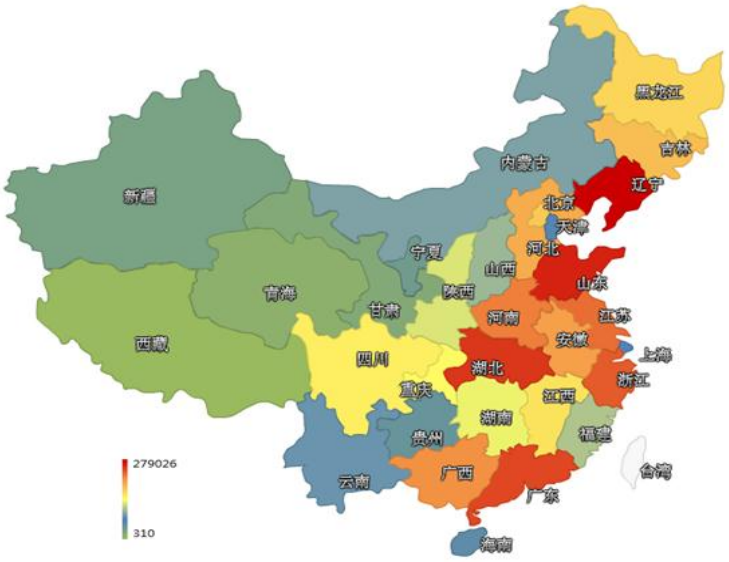
境内感染网络病毒的主机数量	•116.48万	↑53.3%
境内被篡改网站总数 其中政府网站数量	•2305 •47	↓45.1% ↓25.4%
境内被植入后门网站总数 其中政府网站数量	•1887 •93	↓33.6% ↓25.0%
针对境内网站的仿冒页面数量	•4742	↓2.4%
新增信息安全漏洞数量 其中高危漏洞数量	•177 •104	↓14.1% ↑23.8%

=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 116.48 万个，其中包括境内被木马或被僵尸程序控制的主机约 90.14 万以及境内感染飞客（conficker）蠕虫的主机约 26.34 万。



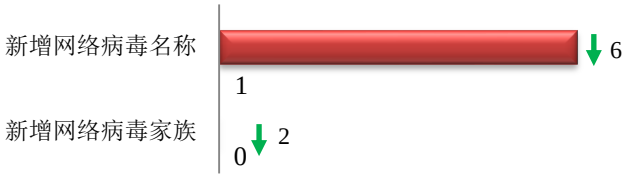


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是辽宁省、山东省和湖北省。

TOP3

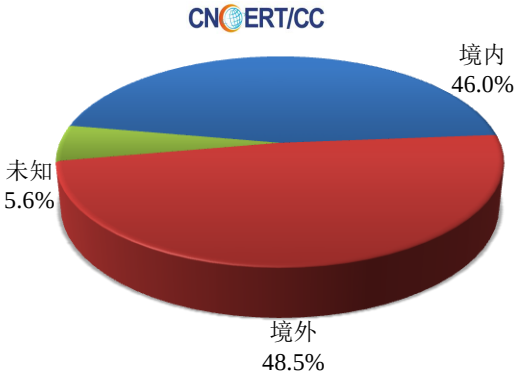
辽宁省	•约27.9万个（约占中国大陆总感染量的31.0%）
山东省	•约9.1万个（约占中国大陆总感染量的10.1%）
湖北省	•约8.7万个（约占中国大陆总感染量的9.6%）

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 1 个，按网络病毒家族统计无新增。

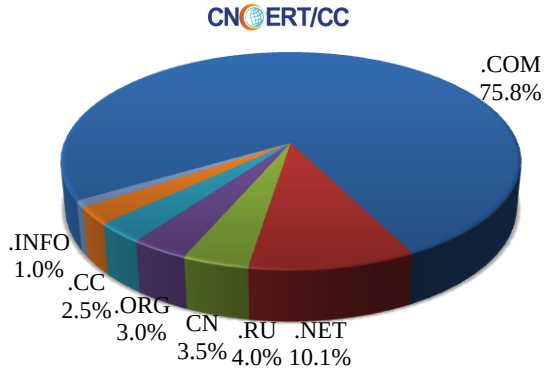


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 198 个，涉及 IP 地址 246 个。在 198 个域名中，有约 48.5%为境外注册，且顶级域为.com 的约占 75.8%；在 246 个 IP 中，有约 27.6%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 52 个 IP。

本周放马站点域名注册所属境内外分布
(10/19-10/25)



本周放马站点域名所属顶级域的分布
(10/19-10/25)



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。

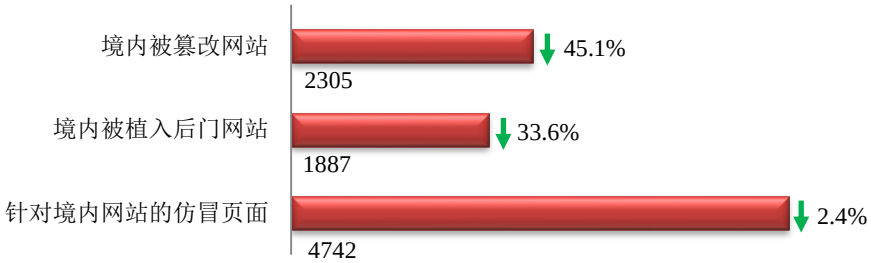
ANVA恶意地址黑名单发布地址

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。

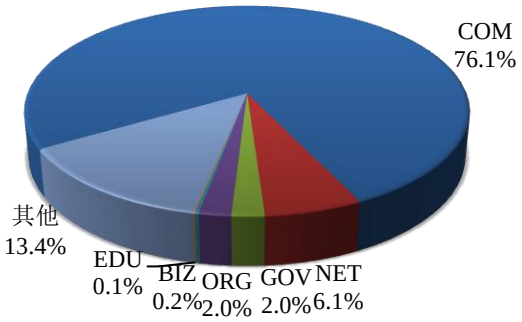
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2305 个；境内被植入后门的网站数量为 1887 个；针对境内网站的仿冒页面数量为 4742。

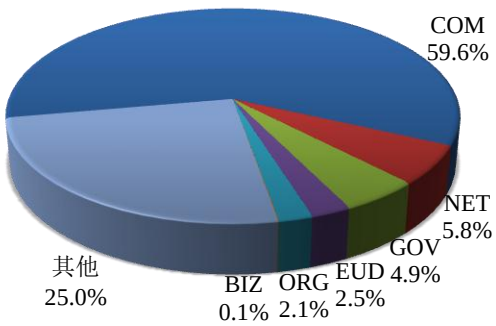


本周境内被篡改政府网站(GOV 类)数量为 47 个（约占境内 2.0%），较上周环比下降了 25.4%；境内被植入后门的政府网站(GOV 类)数量为 93 个（约占境内 4.9%），较上周环比下降了 25.0%；针对境内网站的仿冒页面涉及域名 3881 个，IP 地址 1001 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(10/19-10/25)

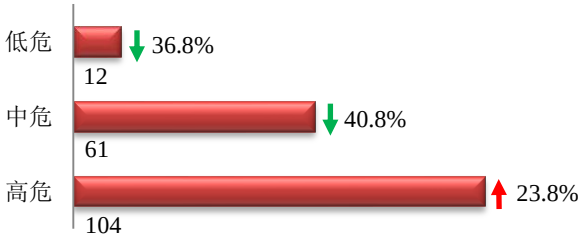


本周我国境内被植入后门网站按类型分布
(10/19-10/25)

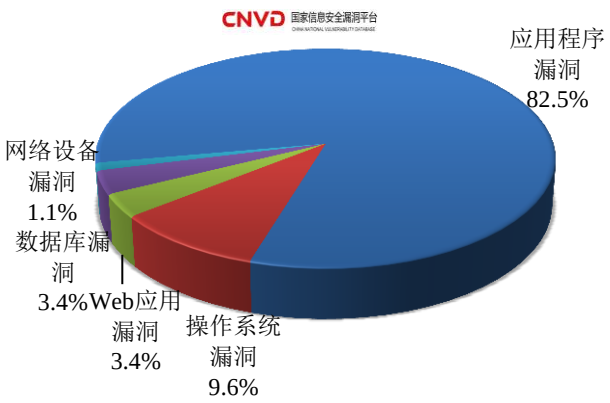


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 177 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
(10/19-10/25)



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

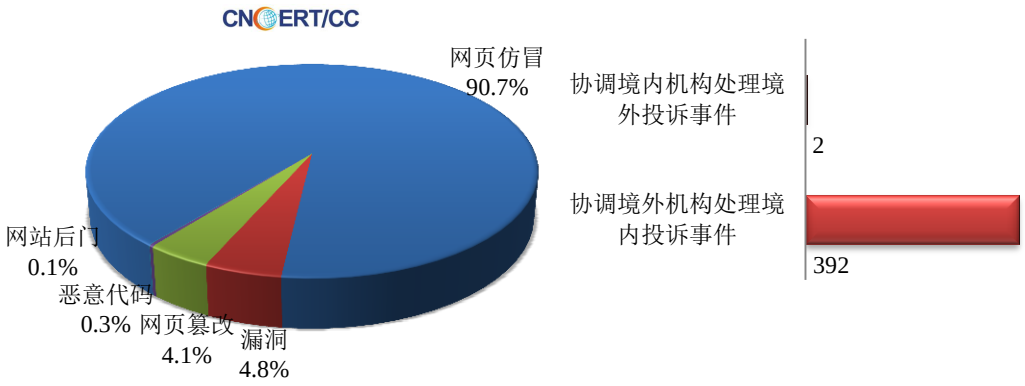
http://www.cnvd.org.cn/webinfo/list?type=4

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 1804 起，其中跨境网络安全事件 394 起。

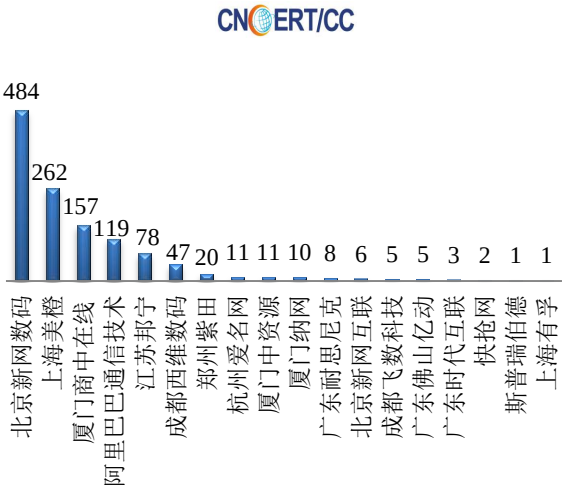
本周CNCERT处理的事件数量按类型分布
(10/19-10/25)



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 1637 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 1251 起和互联网服务提供商仿冒事件 381 起。

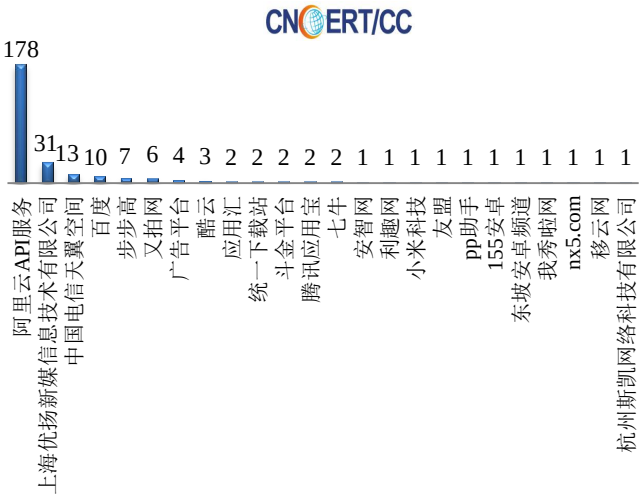
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(10/19-10/25)

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 (10/19-10/25)



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 273 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 (10/19-10/25)



业界新闻速递

1、英媒：中英签订首个网络安全协定

新浪网 10 月 22 日消息 据英国《卫报》报道，当地时间 10 月 21 日，英国首相卡梅伦在同中国国家主席习近平在唐宁街 10 号首相官邸进行会晤后表示，英中两国已经就打击网络犯罪问题签署了一项“高级别安全对话”协议，旨在防止以盗窃知识产权或瘫痪系统为目的的对两国企业的网络攻击。双方将同意既不会监视双方企业的知识产权及机密信息，也不会容忍这一行为。卡梅伦称，这项网络协议将是中国和英国迈向未来更广泛的安全合作的第一步。报道称，这项协议是英国和中国首次在网络安全领域许诺共同合作。

2、英遭遇史上最大黑客攻击 400 万用户数据恐遭泄

凤凰网 10 月 25 日消息 10 月 24 日，英国宽带服务供应商 TalkTalk 表示，该公司受到了一起极其严重的网络袭击，其 400 万用户个人信息可能被“扒光”，这是英国史上最大规模的数据泄露事件之一。据路透社报道，23 日 TalkTalk 公司收到了“未知方”提出的赎金要求。公司称这一“未知方”表示对网络攻击负责并要求公司缴纳赎金，否则公司近 400 万用户包括银行账号和信用卡等信息的具体细节将有曝光风险。电脑专家称 TalkTalk 提供的攻击细节和公共网络数据显示，黑客直接通过 TalkTalk 公司用户网站的漏洞获取了信息，并没有进行内部攻击。路透社援引火眼（FireEye）和速 7（Rapid7）两家网络安全调研机构消息称，在“深网”（Dark Web）的一些网络攻击犯罪论坛上已经开始贩卖部分经济数据样本。而 TalkTalk 公司发言人拒绝评论，称警方正在进行调查中。大多数专家称希望等到警方调查给出更多技术细节在研究攻击方式，以及攻击源头。警方在公布具体情况前可能需要花上数周乃至数月时间。哥本哈根网络法律调查者简·蒙拉得（Jens Monrad）称黑客如果需要增加所偷取的用户数据价值，往往会现在网上公开部分数据样本，以吸引地下犯罪网络的买家，而这些买家则相对也会提高这一价值。苏格兰网络犯罪司的前探员阿德里安·库雷（Adrian Culley）向 BBC 透露称，该起网络攻击像是一起伊斯兰极端组织的行为，但没有提供更多具体线索。

3、美运营商网络存漏洞：影响所有 Android 设备

C114 中国通信网 10 月 22 日消息 卡耐基梅隆大学“公开漏洞数据库”(CERT)上周五表示，AT&T 和 Verizon 对 LTE 网络的配置存在漏洞，可能会导致数百万部手机遭遇窃听、数据欺诈，以及乱收费等风险。这些网络中的 Android 设备风险最大，因为在 LTE 网络中，Android 系统“缺乏适当的授权许可模式”。研究人员指出，最新发现的这些漏洞会影响每一部 Android 设备。T-Mobile 发言人表示，T-Mobile 的用户此前也受到影响，但目前问题已经解决。此外，苹果产品并未受到影响。这一发现最初来自韩国学术界和信息安全研究人员。LTE 技术基于包交换，而非传统的电路交换。这种新的数据传送方法导致了新一类的攻击，尤其是针对会话发起协议(SIP)的攻击。目前，这一协议被广泛用于语音通话和即时通信服务中。研究人员已发现一种方法，利用 SIP 协议的工作方式去进行攻击。攻击者可以获得免费的带宽，去从事数据密集型活动，例如视频通话，同时不产生额外成本。在某些情况下，攻击者可以建立多个 SIP 会话，从而发动拒绝服务攻击。T-Mobile 和 Verizon 的网络已被确认存在风险。研究人员没有对 AT&T 的网络进行全面测试，但他们认为，AT&T 的网络很可能存在风险。利用这样的漏洞，恶意的 Android 应用可以在用户不知情的情况下偷偷拨打电话，从而给用户造成额外的话费，甚至对用户展开窃听。研究人员指出，所有 Android 版本都存在风险。谷歌已表示，将在 11 月的月度安全更新中为 Nexus 设备修复这一问题，但谷歌并未确认，哪些 Android 版本受到了影响。目前也不清楚，其他受影响的 Android 设备将于何时获得补丁，因为这取决于设备厂商和运营商的情况。

4、黑客劫持全球各地闭路电视摄像机到 DDoS 僵尸网络

环球网 10 月 23 日消息 Incapsula 研究报告显示，全球有超过 900 部闭路电视摄像机因为没有设置密码，或者登录凭据薄弱，因此遭到黑客攻击，并加入到一个覆盖全球的 DDoSing 僵尸网络当中。黑客攻击闭路电视监控系统并不困难，一个简单的字典穷举攻击对付这种系统绰绰有余。被攻击的责任要归结到薄弱的 SSH 或 Telnet 口令，有的管理员甚至没有改变默认密码，或让摄像头连接到外部网络。按照 Incapsula 研究显示，所有受攻击的闭路电视系统均运行了 BusyBox，一个专门为物联网打造的精简版 Linux 操作系统。这些物联网设备具有有限内存和 CPU 资源。经由蛮力破解密码登录之后，黑客将针对 ARM 架构运行 BusyBox 的恶意软件放在

系统当中。所有受感染的设备都被用来通过 HTTP GET 请求发动 DDoS 攻击。DDoS 攻击主要针对著名的云服务提供商展开。安全专家们已经记录到每秒发送超过 20000 次 HTTP 请求的设备。另一个设备有受到了多个蛮力攻击，它的登录日志记录来自不同 IP 地址的攻击，这意味着它被黑了不止一次。目前，世界各地安装了超过 2.45 亿个视频监控摄像头。这或许可以解释为什么黑客有这样的胃口。

5、日本两大机场遭黑客攻击 疑为知名黑客组织所为

中新网 10 月 19 日消息 据外媒报道，日本成田机场与中部机场日前曾经遭到黑客攻击。日本千叶县与爱知县警方在调查后发现，攻击这两座机场计算机系统的，可能是知名的国际黑客组织“匿名者”。据悉，成田机场的官方网站，是在这个月 10 日凌晨，无法连入，这一情况持续了大约 8 个小时；而就在同一时间，日本中部机场的计算机系统，也同样受到攻击。所幸是在深夜时分，没有班机起降，因此没有对机场营运造成影响。而“匿名者”组织，先前在推特上曾经发布要攻击成田机场与中部机场的计算机系统，因此日本警方开始调查“匿名者”组织与这两起计算机犯罪事件的相关性。

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：王小群

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82991373