国家互联网应急中心

网络安全信息与动态周报

2018 年第 16 期

4 月 16 日-4 月 22 日

CNCERT/CC

本周网络安全基本态势

境内被木马或僵尸程序控制的主机数量	• 19.8万	↓ 4.2%
境内被篡改网站总数 其中政府网站数量	• 1266 • 33	↑ 29.7% ↓ 2.9%
境内被植入后门网站总数 其中政府网站数量	• 1294 • 36	↑ 12.8% ↑ 28.6%
针对境内网站的仿冒页面数量	• 842	↓ 21.9%
新增信息安全漏洞数量 其中高危漏洞数量	• 248 • 80	↓ 21.5% ↓ 29.2%

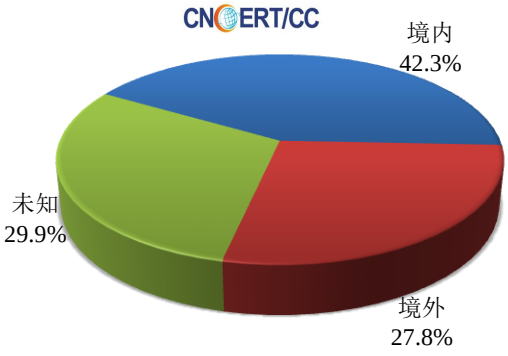
= 表示数量与上周相同　↑ 表示数量较上周环比增加　↓ 表示数量较上周环比减少

本周网络病毒活动情况

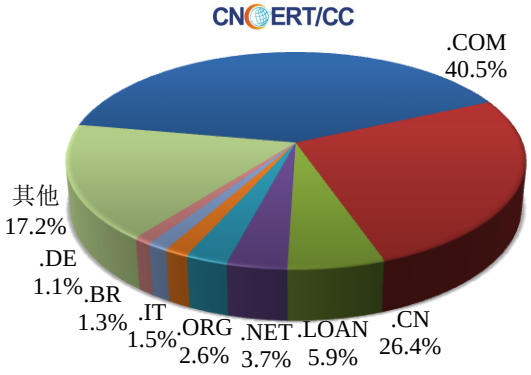
本周，境内被木马或僵尸程序控制的主机数量约为 19.8 万。

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 546 个，涉及 IP 地址 2743 个。在 546 个域名中，有 27.8%为境外注册，且顶级域为.com 的约占 40.5%；在 2743 个 IP 中，有约 43.8%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 44 个 IP。

本周放马站点域名注册所属境内外分布
(4/16-4/22)



本周放马站点域名所属顶级域的分布
(4/16-4/22)



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。

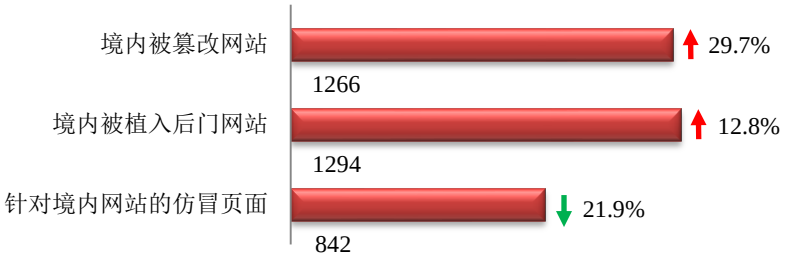
ANVA恶意地址黑名单发布地址

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。

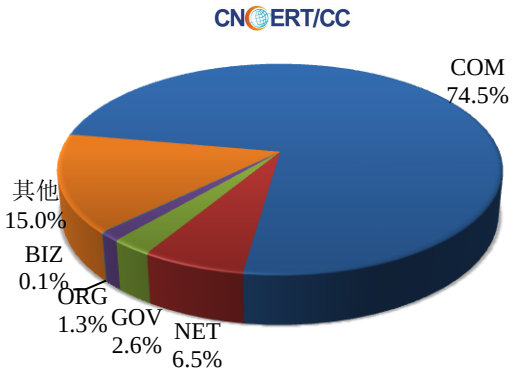
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1266 个；境内被植入后门的网站数量为 1294 个；针对境内网站的仿冒页面数量为 842。

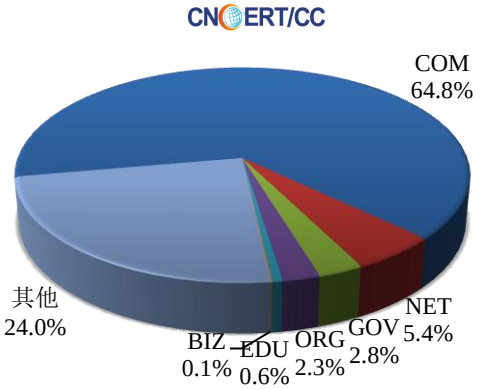


本周境内被篡改政府网站（GOV 类）数量为 33 个（约占境内 2.6%），较上周环比下降了 2.9%；境内被植入后门的政府网站（GOV 类）数量为 36 个（约占境内 2.8%），较上周环比上升了 28.6%；针对境内网站的仿冒页面涉及域名 366 个，IP 地址 153 个，平均每个 IP 地址承载了约 6 个仿冒页面。

本周我国境内被篡改网站按类型分布
(4/16-4/22)

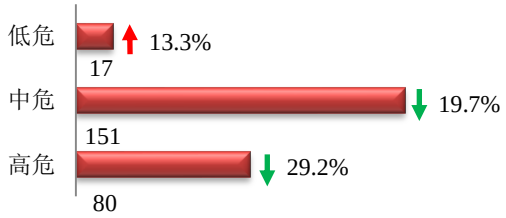


本周我国境内被植入后门网站按类型分布
(4/16-4/22)

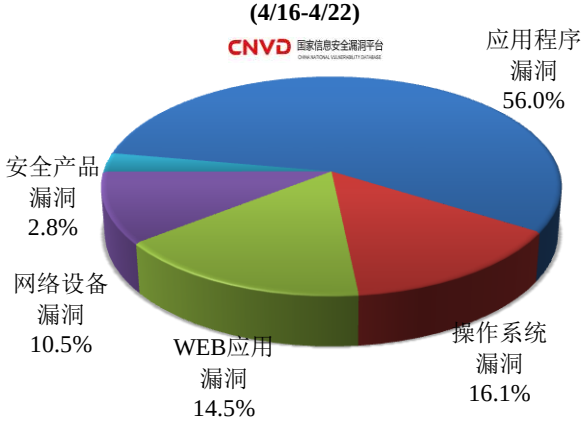


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 248 个，信息安全漏洞威胁整体评价级别为高。



本周CNVD收录漏洞按影响对象类型分布
(4/16-4/22)



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

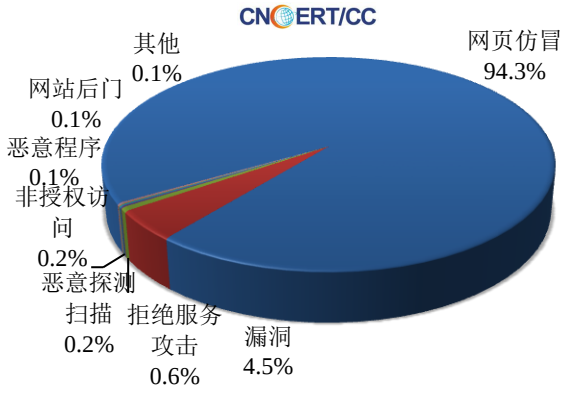
http://www.cnvd.org.cn/webinfo/list?type=4

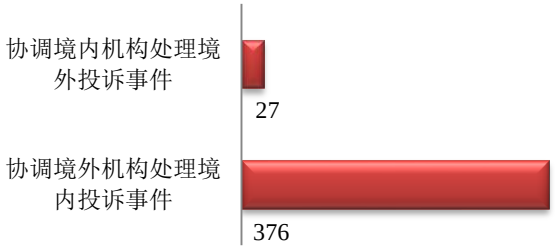
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 1070 起，其中跨境网络安全事件 403 起。

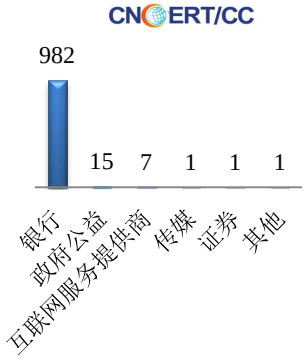
本周CNCERT处理的事件数量按类型分布 (4/16-4/22)



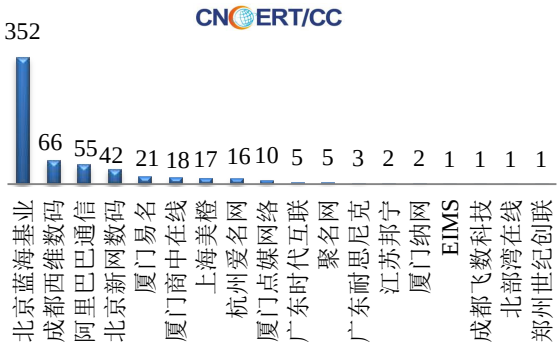


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1007 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 982 起和政府公益仿冒事件 15 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(4/16-4/22)

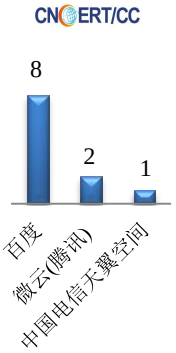


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (4/16-4/22)



本周，CNCERT 协调 3 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 11 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
(4/16-4/22)



业界新闻速递

1、习近平出席全国网络安全和信息化工作会议并发表重要讲话

央广网 4 月 21 日消息 全国网络安全和信息化工作会议 4 月 20 日至 21 日在北京召开。中共中央总书记、国家主席、中央军委主席、中央网络安全和信息化委员会主任习近平出席会议并发表重要讲话。他强调，信息化为中华民族带来了千载难逢的机遇。我们必须敏锐抓住信息化发展的历史机遇，加强网上正面宣传，维护网络安全，推动信息领域核心技术突破，发挥信息化对经济社会发展的引领作用，加强网信领域军民融合，主动参与网络空间国际治理进程，自主创新推进网络强国建设，为决胜全面建成小康社会、夺取新时代中国特色社会主义伟大胜利、实现中华民族伟大复兴的中国梦作出新的贡献。

2、美国能源行业网络安全政策新动向

E 安全 4 月 20 日消息 当地时间 2018 年 4 月 18 日，美国众议院能源和商业小组委员会通过 4 项能源安全法案，旨在提升美国能源部的网络响应能力和参与度，并制定新计划解决电网和管道的安全问题。该小组委员会通过的 4 项法案为：要求美国能源部长里克·佩里制定计划提高美国能源管道和液化天然气设施的物理安全与网络安全（“管道与液化天然气设施网络安全准备法案”）；提出将美国能源部的应急响应和网络安全工作领导权力提至助理部长一级（“能源应急领导法案”）；制定计划帮助私营公共事业公司识别并使用网络安全功能强大的产品（“2018 网络感知法案”）；提出加强公私合作确保电力设施安全（通过“公私合作加强电网安全法案）。美国众议院能源和商业委员会主席格雷戈·沃尔顿表示，这些法案提出“采取可行的措施”，确保美国能源部能有效执行应急和安全活动，并确保美国能源供应安全可靠。这些法案现已提交到美国众议院能源与全体商业委员会投票，此后再提交到众议院。

3、英国 GCHQ 主任确认对伊斯兰国发起了重大网络攻击

HackerNews.cc4 月 17 日消息 据外媒近日报道，英国情报机构 GCHQ 总监 Jeremy Fleming 于上周宣布，英国已经针对伊斯兰国（IS）恐怖组织发起了重大网络攻击。Fleming 在曼彻斯特举行的网络英国会议上表示，这些行动为联军镇压 Daesh 的宣传活动做出了巨大贡献，比如阻碍了其协调攻击的能力，并保护了战场上的联军部队。据悉，这次袭击是 GCHQ 与英国国防部合作发起的，他们针对伊斯兰国进行了分布式作战。GCHQ 认为，该网络攻击事件是第一次系统而持续地降低对手的在线行动，并且也作为了更广泛的军事行动的一部分。虽然 Fleming 并没与透露太多有关攻击行动的细节，但是他表示这场攻击活动显示了有针对性和有效的攻击性网络方式，并且认为此次攻击事件的成功对反对滥用技术传播宣传的威胁做出了表率。

4、微软 Facebook 等科技巨头缔结公约 不协助政府打网络战

凤凰网 4 月 18 日消息 据路透社北京时间 4 月 18 日报道，当地时间星期二，微软、Facebook 和另外逾 30 家全球科技公司公布了一项公约，不帮助任何政府发动网络攻击。《网络安全科技公约》要求缔约公司保护所有客户不会受到网络攻击。微软总裁布拉德·史密斯（Brad Smith）领导了组建该联盟的工作，他表示，2017 年破坏性的网络攻击表明，科技行业需要采取更有操守和更有效的措施，联合起来保护全球客户的安全。《网络安全科技公约》还承诺将在科技行业内建立新的正式和非正式合作关系，与安全研究人员合作，共享威胁信息，协调漏洞披露行为。除微软和 Facebook 外，签署《网络安全科技公约》的另外 32 家科技巨头包括思科、Juniper Networks、甲骨文、诺基亚、SAP、戴尔，以及网络安全公司赛门铁克、FireEye 和趋势。没有签署这一公约的知名美国科技公司包括亚马逊、苹果、Alphabet 和 Twitter。

5、泰国最大 4G 移动运营商 TrueMove H 遭遇 AWS S3 存储桶数据泄露

HackerNews.cc4 月 16 日消息 据外媒 4 月 15 日报道，泰国最大 4G 移动运营商 TrueMove H 于近期遭遇了数据泄露，一位操作人员将 AWS S3 存储桶中总计 32 GB 的 46000 人数据公开在互联网上，其中包括身份信息、护照和驾驶执照等数据。目前根据 TrueMove H 发布的声明显示，其子公司 I True Mart 遭受到了此次泄露的影响。安全研究人员 Niall Merrigan 透露像 bucket stream 和 bucket-finder 这样的工具允许扫描互联网来打开 S3 AWS buckers，例如此次事件，Merrigan 使用了“bucket-finder”工具来发现打开 TrueMove H 的 S3 桶。Merrigan 表示他已将这一问题告知 TrueMove H，但该操作人员并没有做出回应。

6、美国数据公司泄露 4800 万网民资料：包含详细个人信息

新浪网 4 月 19 日消息 北京时间 4 月 19 日早间消息，一家鲜为人知的美国数据公司在用户毫不知情的情况下，通过 Facebook、LinkedIn、Twitter 和 Zillow 等社交网络收集和合并大量用户数据，构建 4800 万人的个人资料，并且一度将其公开泄露出来。这家总部位于美国华盛顿州贝尔维尤的公司名叫 Localblox，他们表示可以“从网络和交换网络中，以多种形式自动爬取、发现、提取、索引、映射和增强数据”。自从 2010 年创办以来，该公司一直在通过 Facebook、Twitter、LinkedIn 等公开数据来源收集信息，制作用户资料。但在今年早些时候，该公司将大量资料数据放在亚马逊 S3 上却没有添加密码，导致任何人都可以下载这些信息。这部分资料标签为 lbdumps，其中包含了一个超过 1.2TB 的文件，上面列出了 4800 万个人用户的信息，全部都是通过公开资料收集后合并起来的。这些数据以 JSON 文件形式存储，可以直接阅读其中的内容。数据中包含姓名、家庭住址、工作信息、职业历史等。

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。截至 2017 年，CNCERT 与 72 个国家和地区的 211 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