国家互联网应急中心

2018 年第 13 期

3 月 26 日-4 月 1 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

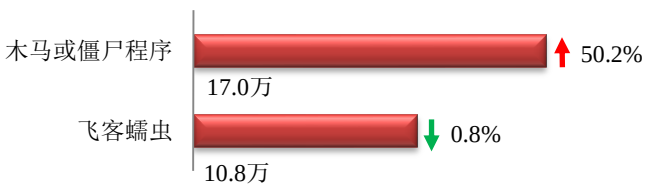
优 | 良 | 中 | 差 | 危

境内感染网络病毒的主机数量	• 27.8万	↑ 25.1%
境内被篡改网站总数 其中政府网站数量	• 746 • 16	↓ 18.5% ↓ 38.5%
境内被植入后门网站总数 其中政府网站数量	• 1032 • 14	↓ 7.1% ↓ 6.7%
针对境内网站的仿冒页面数量	• 1064	↓ 39.8%
新增信息安全漏洞数量 其中高危漏洞数量	• 452 • 134	↓ 7.2% ↓ 22.5%

= 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

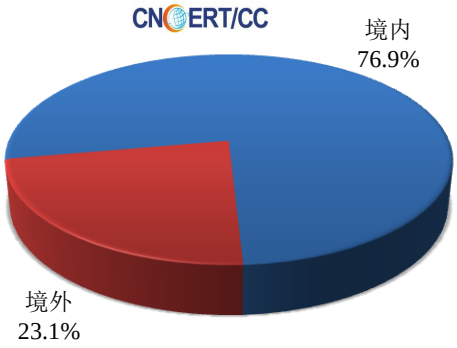
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 27.8 万个，其中包括境内被木马或被僵尸程序控制的主机约 17.0 万以及境内感染飞客（conficker）蠕虫的主机约 10.8 万。

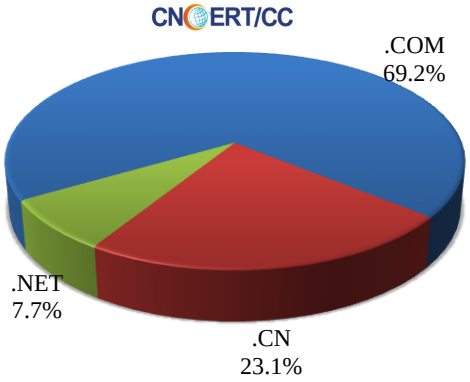


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 13 个，涉及 IP 地址 249 个。在 13 个域名中，有 23.1%为境外注册，且顶级域为.com 的约占 69.2%；在 249 个 IP 中，有约 93.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 2 个 IP。

本周放马站点域名注册所属境内外分布
(3/26-4/1)



本周放马站点域名所属顶级域的分布
(3/26-4/1)



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。

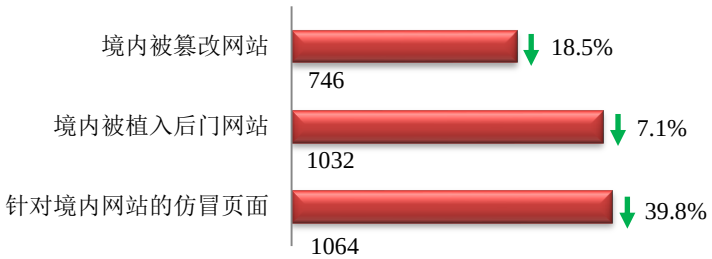
ANVA恶意地址黑名单发布地址

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。

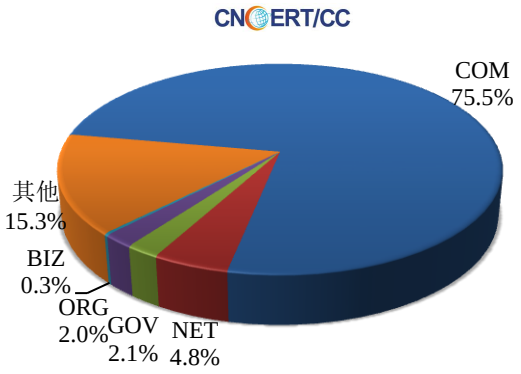
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 746 个；境内被植入后门的网站数量为 1032 个；针对境内网站的仿冒页面数量为 1064。

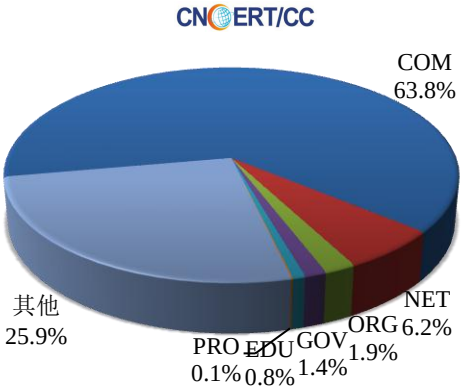


本周境内被篡改政府网站（GOV 类）数量为 16 个（约占境内 2.1%），较上周环比下降了 38.5%；境内被植入后门的政府网站（GOV 类）数量为 14 个（约占境内 1.4%），较上周环比下降了 6.7%；针对境内网站的仿冒页面涉及域名 471 个，IP 地址 163 个，平均每个 IP 地址承载了约 7 个仿冒页面。

本周我国境内被篡改网站按类型分布
(3/26-4/1)

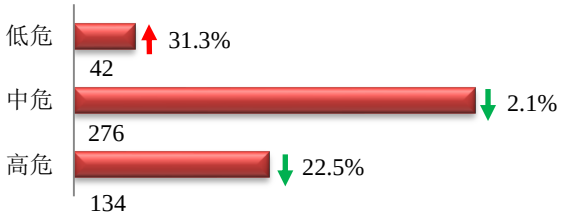


本周我国境内被植入后门网站按类型分布
(3/26-4/1)

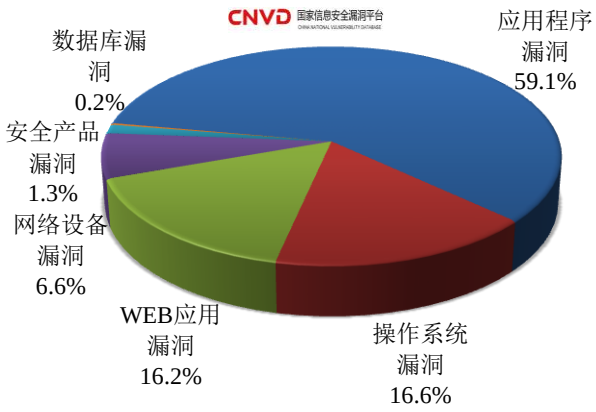


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 452 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
(3/26-4/1)



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

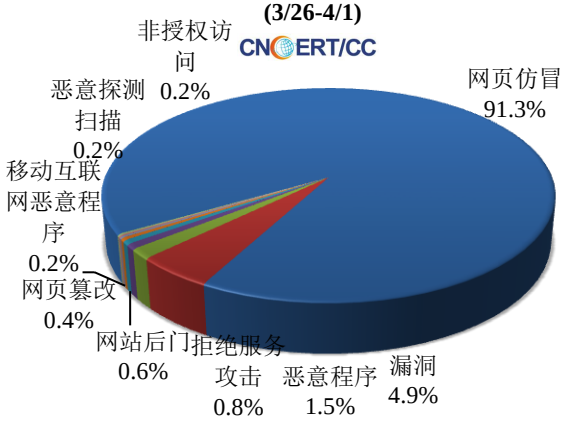
http://www.cnvd.org.cn/webinfo/list?type=4

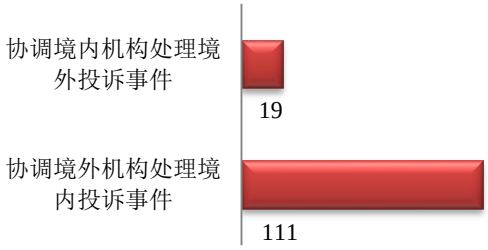
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 529 起，其中跨境网络安全事件 130 起。

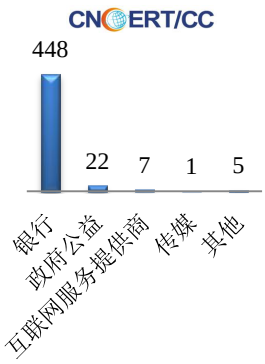
本周CNCERT处理的事件数量按类型分布 (3/26-4/1)



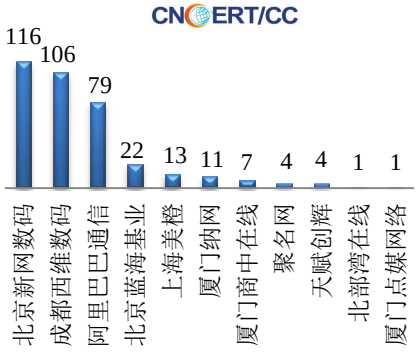


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 483 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 448 起和政府公益仿冒事件 22 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(3/26-4/1)



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 (3/26-4/1)



本周，CNCERT 协调 1 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 1 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
(3/26-4/1)

业界新闻速递

1、英国发布“网络安全出口”战略

E 安全 3 月 29 日消息 英国 2018 年 3 月 26 日正式发布网络安全出口战略，旨在支持对外贸易。该国正在积极宣传自身网络技术实力，并通过新的网络安全出口战略促进面向其它国家的出口规模，从而应对自身与俄罗斯间的冲突。英国认为自身网络能力与强大的安全方法拥有着重要的市场价值，可将其作为面向合作伙伴的有力援助，有望助力自身的资产出口活动。3 月 26 日，该国国际贸易部长利亚姆·福克斯博士正式启动英国政府新的网络安全出口战略，旨在利用网络安全专业知识增强自身以及伙伴国家的网络防御能力。此次公布的新战略，旨在获得更可观的市场份额，此外还将支持 2016 年出台的国家网络安全战略的相关工作。此前公布的这项战略包括提供 19 亿英镑投资以强化英国网络能力，其中大部分将被交付至由英国政府通讯总部（简称 GCHQ）拆分而来的英国国家网络安全中心。

2、1.5 亿用户资料泄露！美体育用品巨头手机应用程序遭黑客入侵

环球网 3 月 31 日消息 当地时间 3 月 29 日，美国知名体育运动品牌安德玛（Under Armour）发布消息称，该公司一款手机应用程序遭黑客入侵，共计 1.5 亿个人账号被攻破。从潜在受害者规模来看，此次事件已算得上网络历史上最为严重的黑客攻击事件之一。据彭博社 30 日报道，遭泄露的用户信息主要包括 App 用户名、密码和个人电子邮箱地址，但不包括个人银行卡号码和社保号码。波士顿东北大学网络安全专家科达表示，对于不法分子而言，个人电邮也是极具价值的信息;在不受约束的暗网体系内，该类信息通常会被竞价最高的买主拍走。遭黑客入侵的是安德玛公司旗下一款饮食、健身辅助应用程序 My Fitness Pal。致力于打造全球最大健身信息数据库的安德玛在 2015 年以 4.75 亿美元收购了这款 AppMy Fitness Pal，后者当时已拥有约 8000 万用户。安德玛公司声明称，已配合执法部门处理此案，同时聘用安全公司展开独立调查。29 日，安德玛通过电邮和 App 消息提醒用户立刻更改密码。

3、继孟加拉央行后 马来西亚央行又被黑客盯上

腾讯网 3 月 30 日消息 据外媒报道，马来西亚央行周四宣布，它近日挫败了一次通过在 SWIFT 交易平台上发送欺诈性信息来盗窃资金的网络攻击。这是全球金融机构遭遇的一系列电子抢劫案件中的最新案例，也是继 2016 年孟加拉央行失窃 8100 万美元资金后发生的第二起针对国家央行的网络攻击事件。马来西亚央行表示，这起网络攻击事件发生在本周二，没有造成任何资金损失。马来西亚央行称，此次网络攻击涉及到欺诈性 SWIFT 转账请求，这给全球金融机构敲响了警钟，敦促它们加强安全防范。目前还不清楚此次网络攻击的幕后操纵者是谁，也不知道他们是如何侵入银行的 SWIFT 服务器，但该事件可能会引发加强安全防护的进一步呼吁。马来西亚央行表示，央行的其他支付和结算系统没有因为此次网络攻击受到干扰。该银行表示，它正在同当地和国际执法机构合作进行调查。

4、印度考题外泄百万学生重考 当局誓言加强网络安全

中新网 3 月 30 日消息 据外媒报道，印度发生高中考试试题在考前外泄事件，迫使数百万名高中生必须重考数学和经济学。3 月 29 日，印度当局誓言将加强网络安全，避免类似事件再次发生。据报道，印度人力资源发展部长贾瓦德卡尔表示，相关当局正在进行调查，了解数学和经济学的试卷，是如何在考试前外泄，并通过通讯软件 WhatsApp 转传。贾瓦德卡尔称，“干下这件事情的罪犯不会被饶恕，我相信警方很快会逮到这些人。我向大家保证，我们将进一步改善这个系统并让它万无一失。”印度主要反对派国大党党魁拉胡尔· 甘地，藉由这次考题外泄事件，再次抨击总理莫迪的政府漠视数字安全。据悉，印度中等教育中央委员会的考试试卷，对希望就读印度最负盛名公立大学的学生们来说至关重要，考题外泄一事因此引发印度各界愤怒。

5、印度电力公司遭遇黑客攻击，勒索 1 RS Core 或 1000 万卢比

HackerNews.cc4 月 1 日消息 上周，黑客攻占了印度 Uttar Haryana Bijli Vitran Nigam（UHBVN）电力公司的计算机系统，窃取了客户的账单数据。攻击者对电力公司进行了勒索，索要一个 1 RS Core 或者 1000 万卢比才肯归还数据，1000 万卢比相当于 15 万美元。据新印度快报报道，黑客在 3 月 21 日凌晨获得了计费系统的访问权，员工在 22 日到公司时，发现他们的电脑上闪烁着赎金信息，要求 1 个 RS Core 来恢复数据。电力公司正在通过日志以及其他来源回复数据。账单数据的丢失意味着电力公司无法对之前的客户用量进行计算。

6、波音遭遇勒索软件攻击，WannaCry 成为最大怀疑对象

HackerNews.cc3 月 30 日消息 据西雅图时报报道，波音公司于本周三遭遇了勒索软件攻击（疑似“WannaCry”），其商用飞机制造总工程师 Mike VanderWel 警告称，该勒索软件正在从波音公司南卡罗来纳州北查尔斯顿的工厂扩散出去，并且可能已经导致 777 的翼梁自动装配工具产线瘫痪。VanderWel 担忧恶意软件可能不仅会感染用于飞机功能测试的设备，也可能扩展到“飞机软件”中。但随后波音在 Twitter 上发表声明说，媒体的报道与真实情况具有一定差距，因为根据波音网络安全运营中心的检测，恶意软件的入侵仅影响到少数系统，并且安全人员也已经采取了补救措施。虽然 WannaCry 偶尔还是会被发现试图传播，但大多数情况下，安全研究人员已经能够有效地拦截这个勒索软件。这就是为什么一年之后，所有发布的补丁程序和 AV 软件都能检测到它。目前，波音公司遭受的勒索软件还没有被 100%确认为 WannaCry，安全人员猜测它也有可能只是

WannaCry 的模仿版。

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：高胜

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158