国家互联网应急中心

2019 年第 17 期
4 月 22 日-4 月 28 日

网络安全信息与动态周报

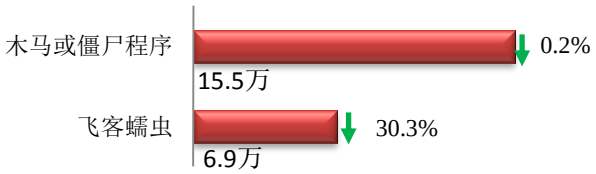
本周网络安全基本态势

境内感染网络病毒的主机数量	• 22.4万	↓ 12.0%
境内被篡改网站总数[1] 其中政府网站数量	• 3681 • 49	↑ 249.2% ↑ 512.5%
境内被植入后门网站总数 其中政府网站数量	• 1728 • 14	↑ 30.8% ↓ 60.0%
针对境内网站的仿冒页面数量	• 1488	↓ 43.7%
新增信息安全漏洞数量 其中高危漏洞数量	• 288 • 104	↑ 25.2% ↑ 8.3%

═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

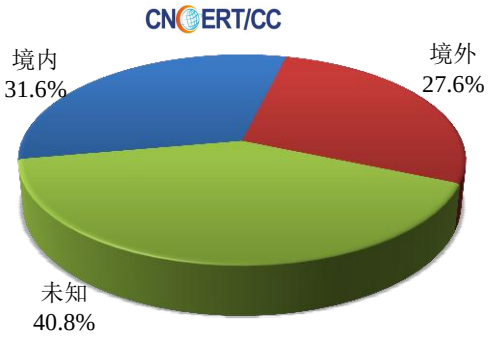
本周境内感染网络病毒的主机数量约为 22.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 15.5 万以及境内感染飞客（conficker）蠕虫的主机约 6.9 万。



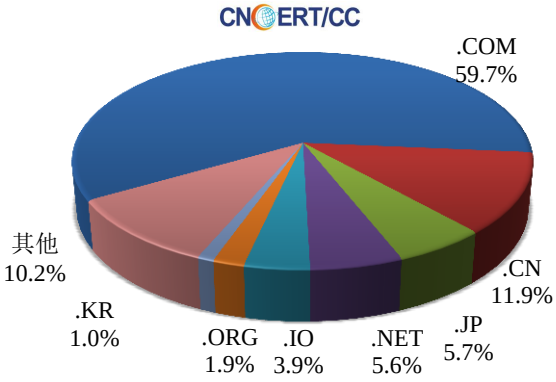
[1]本期境内被篡改网站数量受监测数据范围扩大影响，波动较大

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 6653 个，涉及 IP 地址 3862 个。在 6653 个域名中，有 27.6%为境外注册，且顶级域为.com 的约占 59.7%；在 3862 个 IP 中，有约 45.2%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 387 个 IP。

本周放马站点域名注册所属境内外分布
(4/22-4/28)



本周放马站点域名所属顶级域的分布
(4/22-4/28)



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。

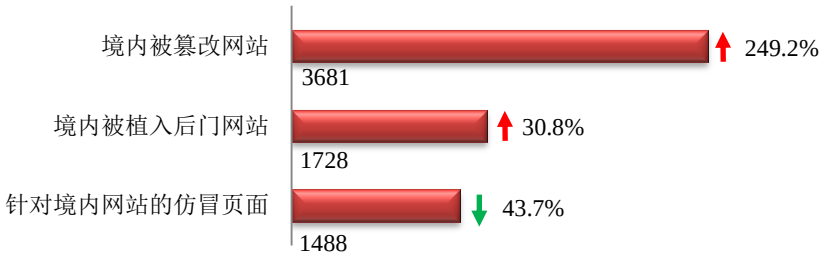
ANVA恶意地址黑名单发布地址

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。

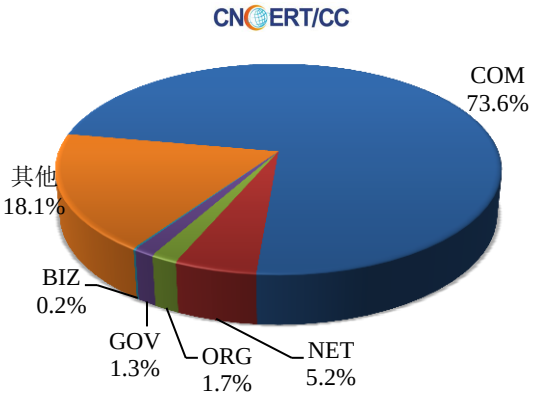
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 3681 个；境内被植入后门的网站数量为 1728 个；针对境内网站的仿冒页面数量 1488 个。

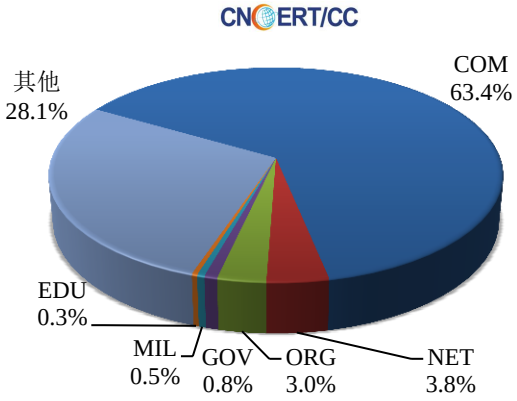


本周境内被篡改政府网站（GOV 类）数量为 49 个（约占境内 1.3%），较上周环比上升 512.5%；境内被植入后门的政府网站（GOV 类）数量为 14 个（约占境内 0.8%），较上周环比下降 60.0%；针对境内网站的仿冒页面涉及域名 526 个，IP 地址 344 个，平均每个 IP 地址承载了约 4 个仿冒页面。

本周我国境内被篡改网站按类型分布
(4/22-4/28)

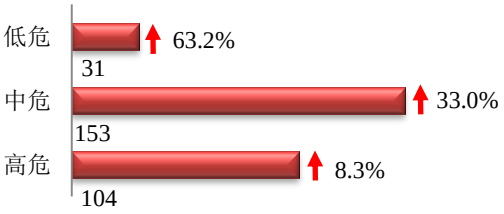


本周我国境内被植入后门网站按类型分布
(4/22-4/28)

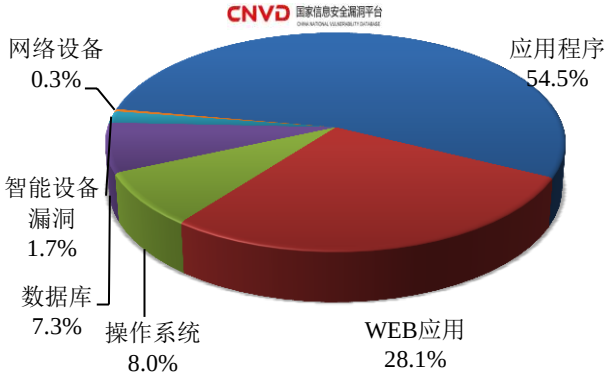


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 288 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
(4/22-4/28)



本周 CNVD 发布的网络安全漏洞中，应用漏洞占比最高，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。

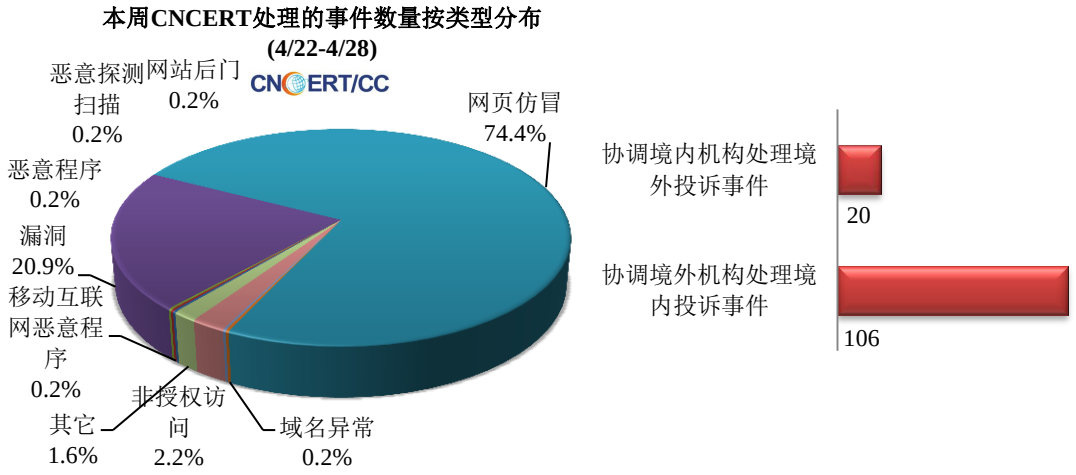
CNVD漏洞周报发布地址

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

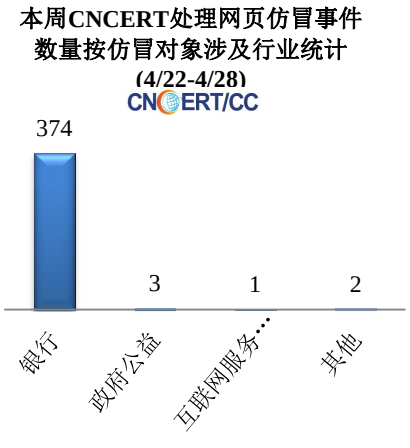
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

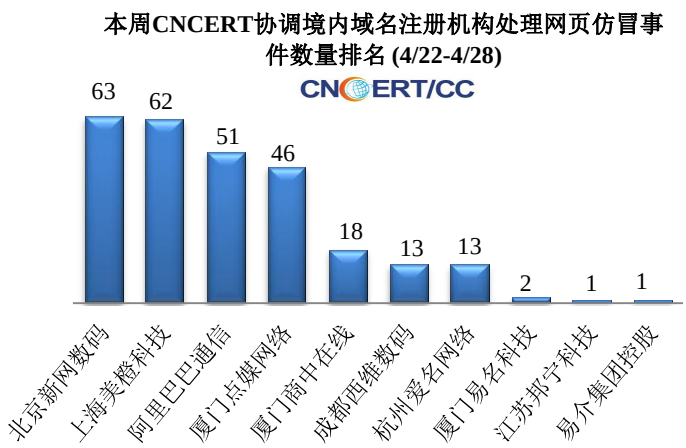
本周事件处理情况

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 511 起，其中跨境网络安全事件 126 起。



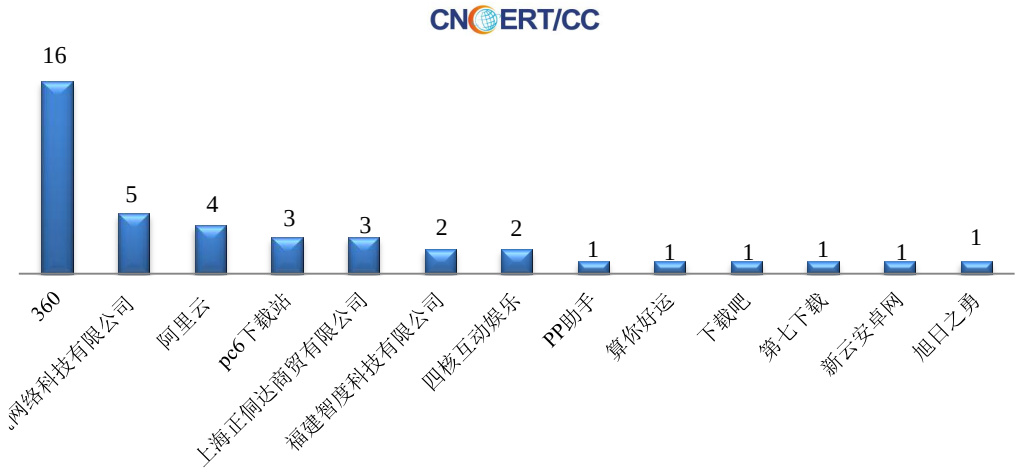
本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 380 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 374 起和政府公益事件 3 起。





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
(4/22-4/28)

本周，CNCERT 协调 13 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 41 个。



业界新闻速递

1、日本拟修改《个人信息保护法》

安全内参 4 月 25 日消息 日本政府的个人信息保护委员会发布了考虑向明年例行国会提交的《个人信息保护法》修正案的中期汇总。主要内容是对企业收集的地址和姓名等个人信息，在个人要求停止用于广告等时，企业有义务同意。修正案若能成为法律，将是 2017 年 5 月全面施行的现行法律中写入每 3 年加以修改后的首次修正。此次中期汇总就 IT 企业收集的个人信息写明，“关于停止利用，有必要探讨拓展个人权利范围的方法”。有关网上过去发布的照片以及犯罪历史的搜索结果等，让网络运营商删除记录的“被忘却的权利”是否写入修正案，则将继续展开讨论。企业合法收集的地址和姓名等个人信息被广泛用于发送广告信件和市场调查等。当个人要求删除数据时，现状是由运营商自己决定，但修正案则规定有义务妥善应对。预计企业根据用户数据发布广告也将受到限制。届时普通消费者可以不必看到感到不愉快的广告等，更容易管理关乎自己的数据。成为监管对象的企业不仅是日企，谷歌和亚马逊等被称为“GAFA”的跨境巨型 IT 企业也被设想在内。日本政府还在讨论建立机制，让据点在海外的企业也适用日本法律。

2、欧洲大型制造企业遭勒索软件攻击

E 安全 4 月 26 日消息 欧洲最大的制造企业之一、在美国设有分支机构的 Aebi Sschmidt 的系统遭勒索软件攻击。Aebi Sschmidt 的业务主要为建造机场和制造公路养护车辆。据称，公司在网络安全事件发生后中断了运营。该公司整个国际网络的系统都崩溃了，其中受到破坏最严重的是瑞士总部。此外，公司的电子邮件服务器

也受到了严重影响。尽管该公司尚未公开承认遭遇勒索软件攻击，但该公司一些员工已证实了这一点。

3、Docker Hub 遭入侵 19 万帐号被泄露

cnBeta.COM4 月 27 日消息 美国当地时间周五晚上，有开发者表示收到来自 Docker 的官方邮件，邮件内容显示由于 Docker Hub 遭受非法入侵，已导致 19 万个帐号的敏感数据被泄露，这些数据包括小部分用户的用户名和哈希密码，以及用于自动构建 Docker 镜像而授权给 Docker Hub 的 GitHub 和 Bitbucket token。按照 Docker 的官方说法，在黑客入侵 Docker Hub 后的短时间内就发现了问题，不过仍有 19 万个帐号的数据已遭泄露，大约是总用户数的 5%。Docker 发现问题后立即向用户告知了这一消息，并通知用户重置密码（包括使用其他使用相同用户名和密码的平台）。此外，对于使用了自动构建服务并可能受影响的用户，Docker 已撤销他们的 GitHub token 和访问密钥，并提醒他们重新连接到存储库，然后检查安全和登录日志以查看是否发生了任何异常操作，例如是否存在通过未知的 IP 地址进行任何未经授权的访问。

4、黑客掌控数万个 iTrack 和 ProTrack 账号 甚至可远程关闭汽车引擎

cnBeta.COM4 月 27 日消息 一名黑客成功入侵了两款 GPS 定位追踪应用，从而让他监控数万辆汽车的位置，甚至能够关闭部分汽车的引擎。这名叫做 L&M 的黑客成功入侵了 7000 多个 iTrack 账号以及超过 20,000 个 ProTrack 账户，这两款应用被用于监控和管理车队的。该黑客可以跟踪南非，摩洛哥，印度和菲律宾等少数国家的车辆。根据部分 GPS 定位追踪设备厂商的设定，如果车辆停靠或者车速低于每小时 12 英里就可以进行远程关闭汽车引擎，而黑客在成功入侵之后可以操控擅自关闭这些汽车引擎。

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：饶毓

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158