国家互联网应急中心

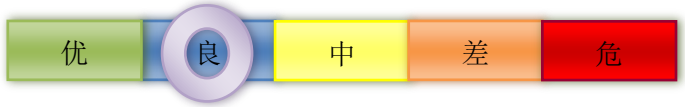
网络安全信息与动态周报

2018 年第 39 期

9 月 24 日-9 月 30 日

CNCERT/CC

本周网络安全基本态势

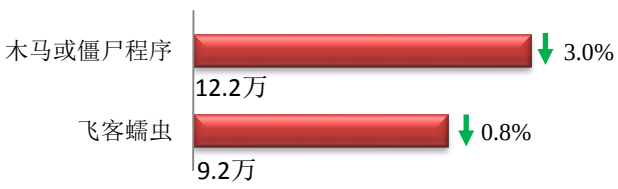


境内感染网络病毒的主机数量	•21.4万	12.1%
境内被篡改网站总数 其中政府网站数量	•382 •30	24.2% 21.1%
境内被植入后门网站总数 其中政府网站数量	•619 •12	9.2% 58.6%
针对境内网站的仿冒页面数量	•1520	38.5%
新增信息安全漏洞数量 其中高危漏洞数量	•267 •93	28.8% 14.7%

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*

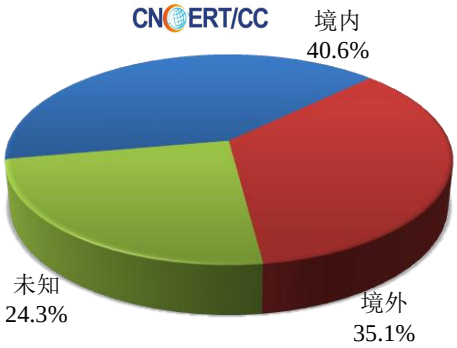
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 21.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 12.2 万以及境内感染飞客（conficker）蠕虫的主机约 9.2 万。

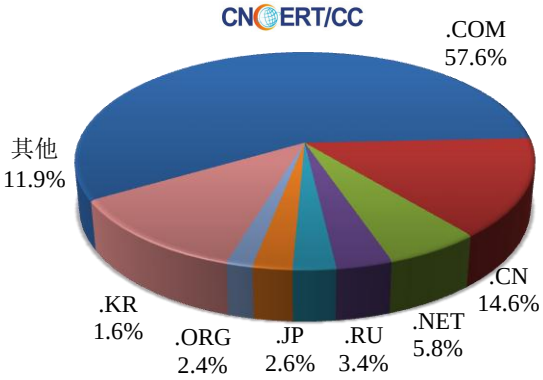


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 2620 个，涉及 IP 地址 55894 个。在 2620 个域名中，有 35.1%为境外注册，且顶级域为.com 的约占 57.6%；在 55894 个 IP 中，有约 35.0%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 372 个 IP。

本周放马站点域名注册所属境内外分布
(9/24-9/30)



本周放马站点域名所属顶级域的分布
(9/24-9/30)



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。

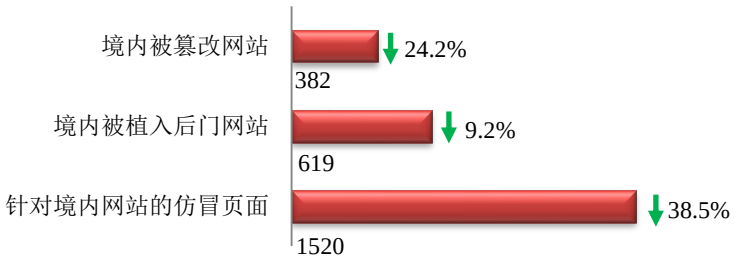
ANVA恶意地址黑名单发布地址

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。

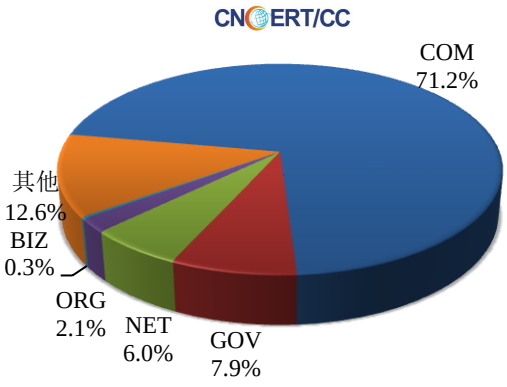
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 382 个；境内被植入后门的网站数量为 619 个；针对境内网站的仿冒页面数量为 1520。

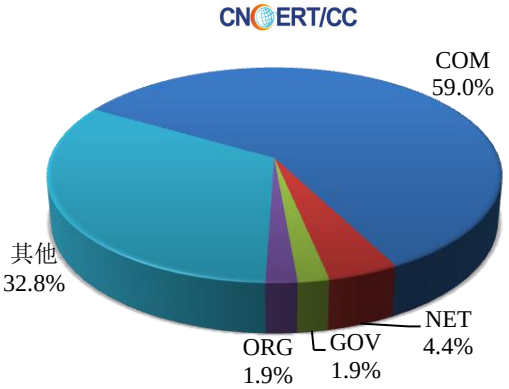


本周境内被篡改政府网站（GOV 类）数量为 30 个（约占境内 7.9%），较上周环比下降了 21.1%；境内被植入后门的政府网站（GOV 类）数量为 12 个（约占境内 1.9%），较上周环比下降了 58.6%；针对境内网站的仿冒页面涉及域名 557 个，IP 地址 264 个，平均每个 IP 地址承载了约 6 个仿冒页面。

本周我国境内被篡改网站按类型分布
(9/24-9/30)

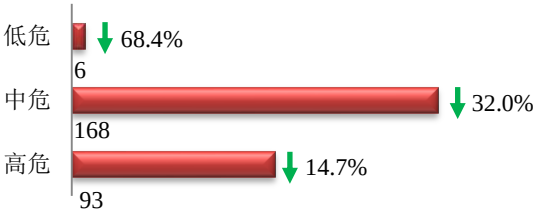


本周我国境内被植入后门网站按类型分布
(9/24-9/30)

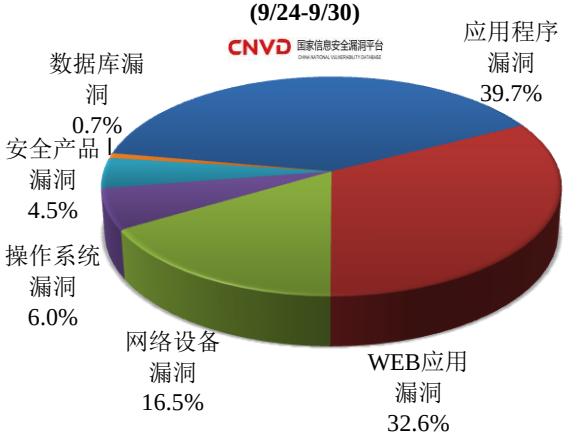


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 267 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
(9/24-9/30)



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 WEB 应用漏洞和网络设备漏洞。

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

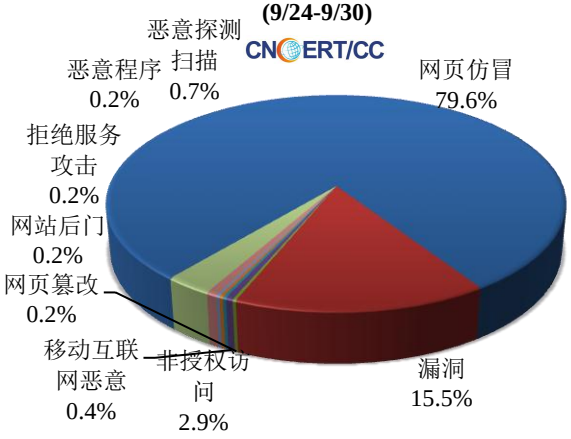
http://www.cnvd.org.cn/webinfo/list?type=4

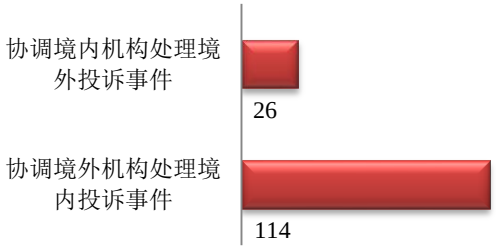
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 446 起，其中跨境网络安全事件 140 起。

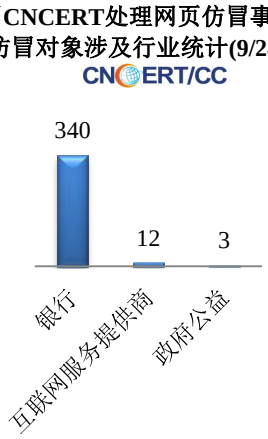
本周CNCERT处理的事件数量按类型分布 (9/24-9/30)



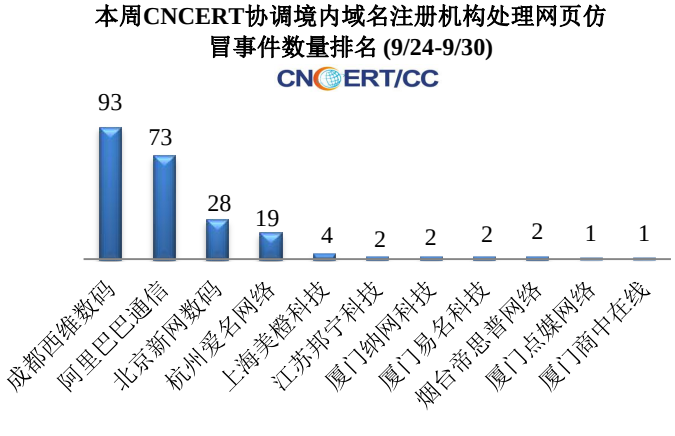


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 355 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 340 起和互联网服务提供商仿冒事件 12 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(9/24-9/30)

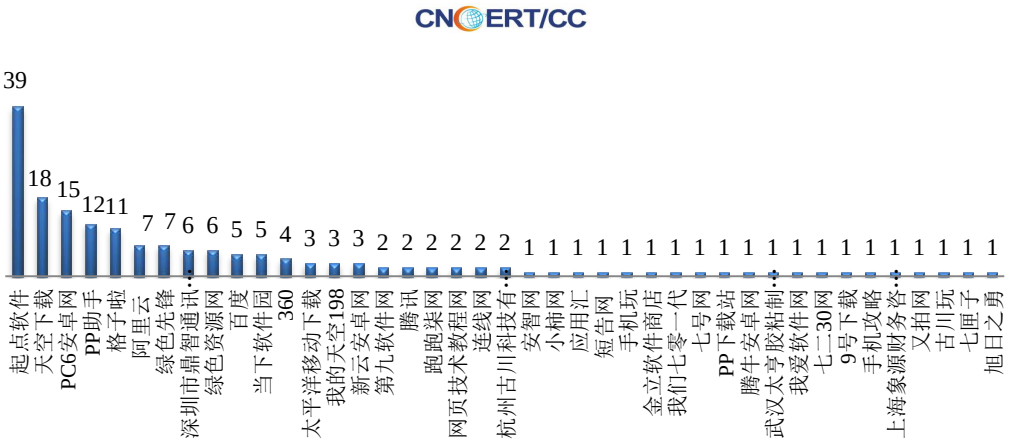


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (9/24-9/30)



本周，CNCERT 协调 41 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 176 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
(9/24-9/30)



业界新闻速递

1.美国白宫发布《量子信息科学国家战略概述》

E 安全 9 月 27 日讯 当地时间 9 月 24 日，美国白宫科技政策办公室（OSTP）国家科学技术委员会（NSTC）发布《量子信息科学国家战略概述》（下称《概述》）。白宫方面认为，量子信息科技（QIS）将引领下一场技术革命，给国家安全、经济发展、基础科研等带来重大变革。《概述》系统性地总结了量子信息科学带来的挑战、机遇，以及为维持和扩大美国在 QIS 领域的领导地位应做出的努力。

另外，美国能源部（DOE）宣布为量子信息科学（QIS）这一重要新兴领域的 85 个研究奖项提供 2.18 亿美元的资助。

2.美国联邦通讯委员会（FCC）投票消除 5G 部署监管障碍

新浪科技讯 北京时间 9 月 30 日消息，特朗普政府周五表示，希望为加快部署 5G 网络扫清障碍。这项技术有望为多个行业带来一场革命。美国联邦通讯委员会（FCC）主席阿基特·派（Ajit Pai）在一次白宫峰会上表示，“美国在 5G 技术上的领导力是获取经济增长和竞争力的必要条件。”

他还表示，5G 网络将会消除无线技术创新所面临的速度和容量局限，这种技术将比目前的网络快 100 倍。“请求数据的设备与网络的响应之间的延迟时间将会缩短到目前的十分之一。”他说，“当今的无线网络支持每平方公里 1000 台联网设备，5G 则能支持 100 万台，”并将最终实现远程外科手术这样的应用。

美国政府官员对这项技术寄予厚望，认为它有望创造 300 万新的就业岗位和 2750 亿美元私有投资，并新增 5000 亿美元经济增长。

5G 网络目前处于最后测试阶段，需要依靠密集的小型天线和云来提供比现有 4G 网络快 50 倍或 100 倍的

网速，并为许多行业充当重要基础设施。

美国国会和监管者还在努力释放更多无线频谱，以供 5G 网络使用，并将改善其他监管措施，方便企业部署光纤网络。

除了大幅加快网速外，5G 还将允许交通网络与无人驾驶汽车和联网汽车相连，而新的无线传感器也可以提供实时健康监测和其他先进的应用。

白宫国家经济委员会主任拉里·库德洛周五表示，5G 竞赛将会“主要通过自由企业、自由市场经济来取胜”。

无线行业组织 CTIA 代表 Sprint、AT&T、三星和英特尔等众多企业的利益，他们在此次峰会结束后的声明中表示：“我们完全同意政府、FCC 和国会领导人的观点，美国通过自由市场在 5G 领域取得的领导地位对我们的经济、私有投资和未来创新至关重要。”

FCC 周三投票消除了 5G 部署的监管障碍。阿基特·派表示，这些措施将给各个城市针对小型基站收取的费用制定上限，并要求地方政府积极审批申请。

阿基特·派还表示，5G 网络需要 80 万个基站，多数都是跟背包大小相仿的小型基站，大约达到现有数量的 4 倍。

3.加州通过物联网网络安全法 有专家质疑其进步意义

新浪科技讯 北京时间 9 月 29 日早间消息，加州州长杰里·布朗（Jerry Brown）在新的网络安全法上签字，这项法律覆盖智能设备，加州成为美国第一个拥有物联网网络安全法的州。法案编号 SB-327，去年制定，8 月末在州参议院获得通过。从 2020 年 1 月 1 日开始，制造商如果制造直接或者间接连接互联网的设备，必须植入“合理”的安全技术，预防未授权访问、修改、信息披露。如果设备可以用密码从本地局限网外访问，必须为每一台设备设立一个独特密码，或者强迫用户在第一次连接时设置密码。这样一来就不会有一般默认凭证，黑客难以猜测。关于新法案有人赞扬，有人批评，赞扬者认这是通往正确方向的第一步，而反对者则认为法案含糊不清。网络安全专家罗伯特·格雷厄姆（Robert Graham）认为，它让安全问题倒退，只是一味增加好的东西，而没有尽力剔除坏的东西。关于密码要求，格雷厄姆赞赏，但是他认为没有覆盖多种多样的身份认证系统，有些系统可能叫作密码，有些可能不叫密码，因为规定不明确，制造商可能会给设备留下安全漏洞。

4.Facebook 发现安全漏洞：黑客可控制 5000 万用户账号

新浪科技讯 北京时间 9 月 29 日早间消息，Facebook 周五宣布，该公司发现了一个安全漏洞，黑客可利用这个漏洞来获取信息，而这些信息原本可令黑客控制约 5000 万个用户账号。

Facebook CEO 马克·扎克伯格（Mark Zuckerberg）称：“这是个非常严重的安全问题，我们正在非常认真地对待。”

在披露这一消息之前，Facebook 股价已经下跌了 1.5%左右，消息传出后进一步走低，到收盘时下跌 2.59%报 164.46 美元，盘中一度触及 162.56 美元的低点。

Facebook 发布博文称，该公司的工程团队发现，黑客在 Facebook 的“View As”功能中找到了一个代码漏洞。Facebook 之所以能发现这个漏洞，是因为该公司在 9 月 16 日注意到用户活动大增。

View As 功能可让用户看到他们自己的个人资料在 Facebook 平台其他用户眼中是怎样的，而此次发现的漏

洞包含了三个不同的 bug，黑客可利用这个漏洞获取“访问令牌”（access token），从而控制其他用户的账号。

近 5000 万个用户账号的“访问令牌”已被黑客获取，但 Facebook 已对其进行了重置。在过去一年时间里，Facebook 还已对另外 4000 万个使用 View As 功能的用户账号的“访问令牌”进行了重置，以此作为预防措施。也就是说，Facebook 总共已对 9000 万个用户账号进行了重置，在截至 6 月 30 日的 22.3 亿名 Facebook 活跃用户总数中所占比例约为 4%。

在“访问令牌”被重置后，用户需在登录时重新输入密码，此外还将在“信息流”（News Feed）中收到通知说明。

另外，Facebook 还将暂时关闭 View As 功能，将对其安全性进行审查。Facebook 在美国当地时间周四晚上称其已经修复了这个漏洞，并已通知美国联邦调查局（FBI）和爱尔兰数据保护委员会（Irish Data Protection Commission）等执法机关，目的是解决任何有关一般数据保护条例（GDPR）的问题。

5.跨境时尚电商 SHEIN 数据泄露 影响 642 万用户

E 安全 9 月 27 日讯 跨境时尚电商 SHEIN 上周宣布了一项安全漏洞，这项漏洞自 2018 年 6 月就存在，直到 8 月 22 日终于被发现。不知名的黑客在此期间窃取了该公司近 650 万客户的个人身份信息（PII）。入侵者设法访问客户的电子邮件地址和加密的在线商店帐户密码。9 月，有媒体报道 SHEIN 的日均活跃用户已超过 100 万。

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：王毓骏

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158