国家互联网应急中心

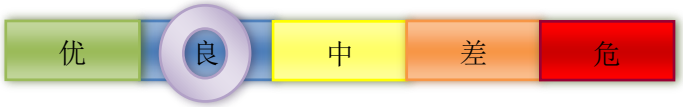
网络安全信息与动态周报

2018 年第 36 期

9 月 3 日-9 月 9 日

CNCERT/CC

本周网络安全基本态势

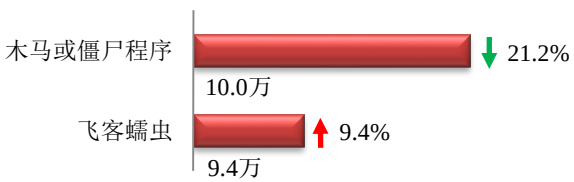


境内感染网络病毒的主机数量	•19.4万	↓ 8.8%
境内被篡改网站总数 其中政府网站数量	•601 •41	↓ 20.9% ↑ 2.5%
境内被植入后门网站总数 其中政府网站数量	•755 •23	↑ 10.7% ↓ 4.2%
针对境内网站的仿冒页面数量	•1763	↓ 7.9%
新增信息安全漏洞数量 其中高危漏洞数量	•424 •177	↑ 19.1% ↑ 39.4%

═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

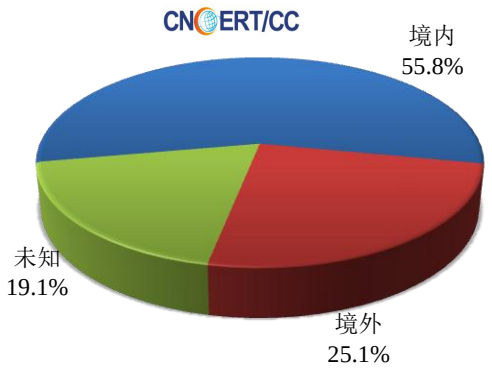
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 19.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 10.0 万以及境内感染飞客（conficker）蠕虫的主机约 9.4 万。

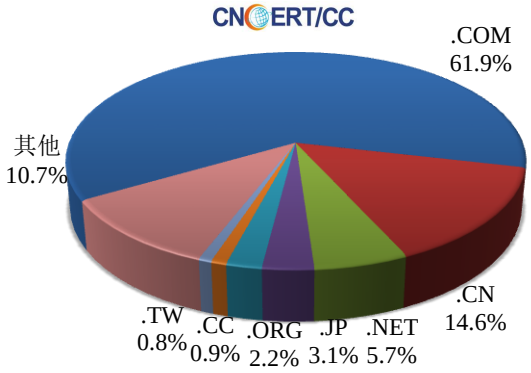


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 3724 个，涉及 IP 地址 178156 个。在 3724 个域名中，有 25.1%为境外注册，且顶级域为.com 的约占 61.9%；在 178156 个 IP 中，有约 32.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 484 个 IP。

本周放马站点域名注册所属境内外分布
(9/3-9/9)



本周放马站点域名所属顶级域的分布
(9/3-9/9)



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。

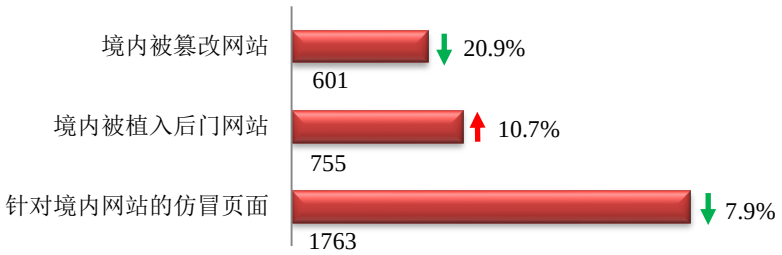
ANVA恶意地址黑名单发布地址

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。

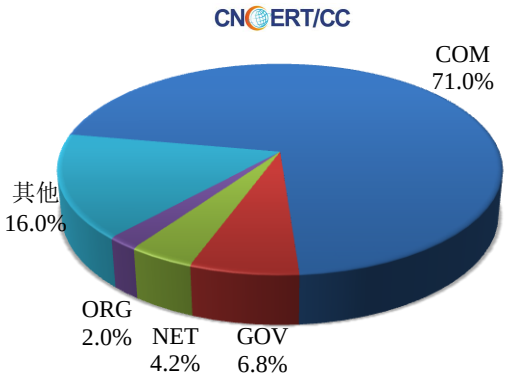
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 601 个；境内被植入后门的网站数量为 755 个；针对境内网站的仿冒页面数量为 1763。

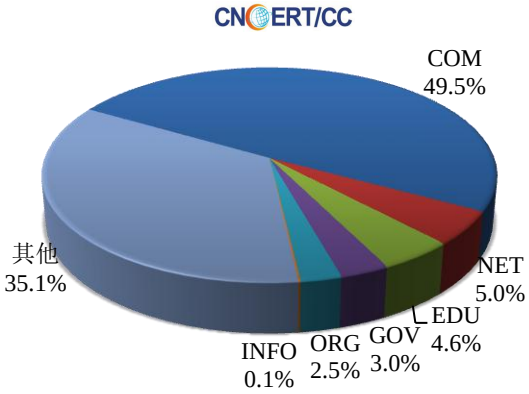


本周境内被篡改政府网站（GOV 类）数量为 41 个（约占境内 6.8%），较上周环比上升了 2.5%；境内被植入后门的政府网站（GOV 类）数量为 23 个（约占境内 3.0%），较上周环比下降了 4.2%；针对境内网站的仿冒页面涉及域名 557 个，IP 地址 270 个，平均每个 IP 地址承载了约 7 个仿冒页面。

本周我国境内被篡改网站按类型分布
(9/3-9/9)

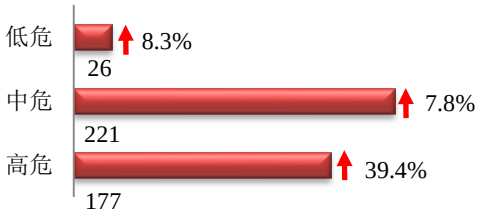


本周我国境内被植入后门网站按类型分布
(9/3-9/9)

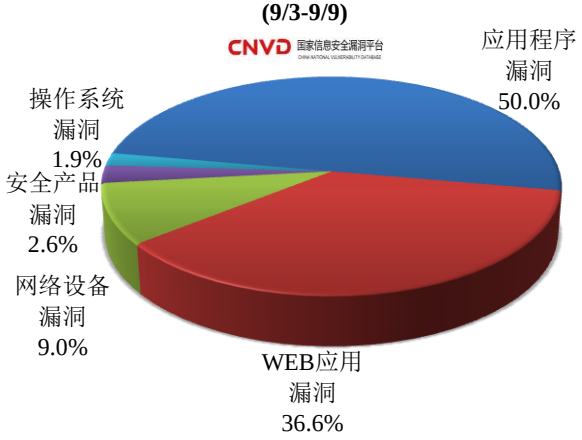


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 424 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
(9/3-9/9)



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

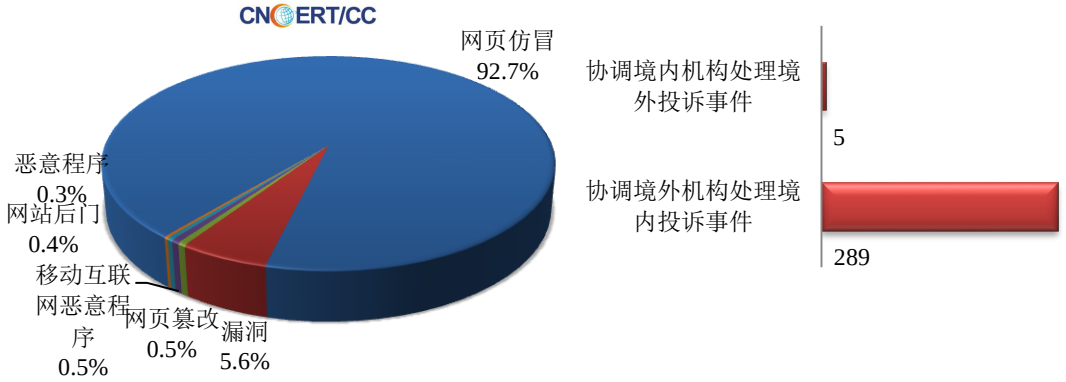
http://www.cnvd.org.cn/webinfo/list?type=4

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

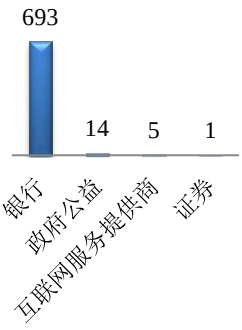
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 769 起，其中跨境网络安全事件 294 起。

本周CNCERT处理的事件数量按类型分布 (9/3-9/9)

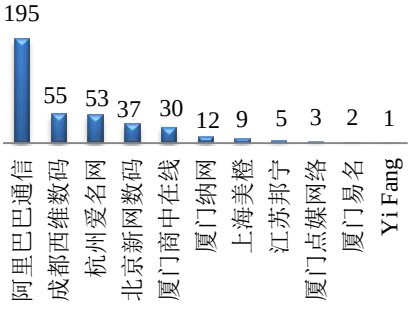


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 713 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 693 起和政府公益仿冒事件 14 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(9/3-9/9)

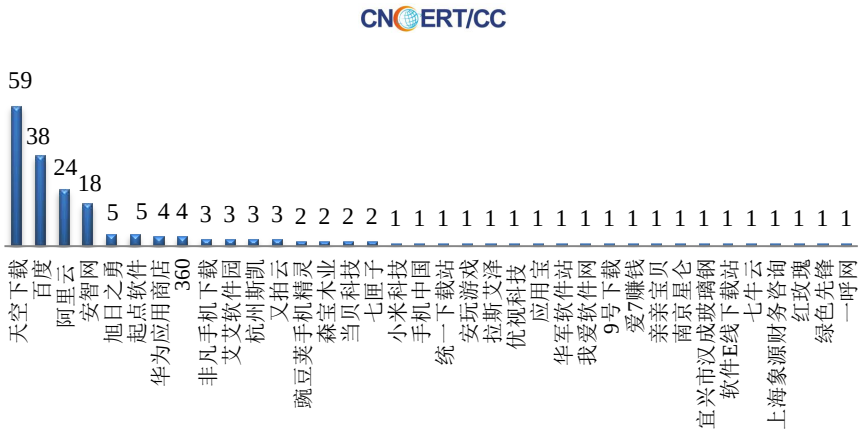


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (9/3-9/9)



本周，CNCERT 协调 36 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 197 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
(9/3-9/9)



业界新闻速递

1、中国工业和信息化部：将尽快出台工业互联网安全相关制度

证券时报网 9 月 4 日消息 上证报报道，中国工业和信息化部 9 月 4 日发布的 2018 年第二季度网络安全威胁态势分析与工作综述提出，将尽快出台工业互联网安全相关制度、标准，组织开展工业互联网安全试点示范工作。下一步将按照相关工作总体部署，组织各地通信管理局、基础电信企业、网络安全专业机构、重点互联网企业和网络安全企业等全力做好重大活动的网络安全保障工作；组织各相关单位开展木马僵尸、病毒、移动恶意程序等相关恶意程序的专项治理工作，降低发生数据泄露、病毒传播和主机被控等网络安全事件的可能；尽快出台工业互联网安全相关制度、标准，组织开展工业互联网安全试点示范工作，加强工业互联网安全解决方案和最佳实践的推广应用。

2、美众议院通过“网络威慑与响应法案”

E 安全 9 月 7 日消息 美国众议院 9 月 5 日通过“网络威慑与响应法案”，其旨在阻止外国政府对美国关键基础设施发起黑客攻击。该法案呼吁美国总统识别参与国家支持型黑客攻击，对美国利益构成严重威胁的个人和组织，并对其实施制裁。

3、美国 NIST 联合 DHS 发布第一份防范 BGP 劫持的安全标准草案

E 安全 9 月 11 日消息 美国国家标准技术研究所（简称 NIST）与国土安全部（简称 DHS）联合发布关于 GBP 路由来源验证（ROV）标准的全新初稿，此项标准将帮助互联网服务供应商与云服务供应商抵御 BGP 劫持攻击。这项启动于 2017 年 10 月的互联网绑定协议制定工作，目前终于迎来初步成果。上周，NIST 下辖的国家网络安全卓越中心（简称 NCCoE）发布了一份安全标准初稿，此项标准旨在为边界网关协议（BGP）提供保

护。NIST 在本周的一份新闻稿中表示，“本指南中描述的示例方案，旨在通过验证路由来源以保护数据完整性，同时提高互联网流量交流机制的弹性。”“基于此项标准的示例解决方案将被部分或者全部引入商用产品。此外，其还可以作为参考素材，帮助各类组织设计出自己的定制化解决方案。”此份草案目前已经面向公众及私营部门开放，并将在 10 月 15 日之前持续征求改进意见。在此之后，草案将交由 IETF（互联网工程任务组，负责批准各类互联网标准）进行审查与批准。

4、新加坡金融管理局（MAS）为金融机构提出具有法律约束力的网络安全措施

E 安全 9 月 7 日消息 新加坡金融管理局（MAS）提议制定一套具有法律约束力的六项基本网络安全措施要求，以保护金融机构的 IT 系统。这些措施已被纳入现有的 MSA 技术风险管理指南，但 MAS 提议将其变成具有法律约束力的要求。这六项措施包括：及时解决系统安全漏洞，为系统建立并实现强大的安全性，部署安全设备以保护系统连接，安装反病毒软件以缓解恶意软件感染风险，限制使用可修改系统配置的系统管理员账户；以及加强关键系统上系统管理员账户的用户身份验证机制。

5、菲律宾中央银行拟向银行发布网络攻击报告通告

E 安全 9 月 4 日消息 据菲律宾中央银行（BSP）官员透露，该行法律部门正在研究一项拟议规则的细节，其将要求银行尽快上报网络攻击和其他 IT 相关事件。预计 BSP 将于 2018 年 9 月发布通告要求银行遵守这一规则。早些时候，BSP 官员曾表示在与菲律宾银行家协会讨论一项举措，其要求银行在事发后 24 小时或 48 小时内提交网络问题相关报告。BSP 已加强监管并要求银行进一步强化 IT 安全系统，以免沦为网络攻击的受害者。此外，BSP 还对金融机构的 IT 安全强度和风险管理框架进行评级。

6、英美等五眼联盟（Five Eyes）国家发布声明要求科技企业自愿提供后门

cnBeta.COM9 月 4 日消息 美国、英国、澳大利亚、新西兰和加拿大五眼联盟（Five Eyes）国家政府发布联合备忘录，要求各大科技企业向政府提供其加密产品的后门，以供执法部门有能力获得访问权。如果企业拒绝提供，那么这些政府会寻求技术的、执法的、立法机构的或者其它手段，进入加密的设备或者服务。这份声明来自上周召开的五眼联盟（Five Eyes）国家会议。该声明鼓励企业自愿向政府提供后门，如果科技企业拒绝并且阻挠，政府将采用强制措施集中力量进行加密破解。目前阶段，要求企业提供后门的请求更像是愿望，而非强制命令或威胁。但声明中提到政府和立法者在破解加密遭遇到了更大的反抗运动，则被视为对执法行为的阻挠。未来不排除将要求企业提供加密信息的请求直接升级为法律行动的可能。

7、英航网站遭黑客攻击 38 万笔用户信用卡数据外泄

中新网 9 月 7 日消息 据“中央社”报道，英国航空（British Airway）9 月 6 日表示，8 月 21 日到 9 月 5 日期间客户订票的个人资料与财务明细遭黑客攻击，大约 38 万笔通过信用卡支付的数据外泄。英航在一项声明指出，正在紧急调查英航网站与手机 APP 遭骇事件，泄漏数据包括顾客订票的个人资料与财务明细，但不包括护照与旅程数据。英航说，个资泄漏问题已经解决，网站目前运作正常。公司已经通知警方与主管当局。英航为这起资料外泄事故致歉，并建议如客户担心受影响，请尽快与自身的银行或信用卡公司联系，依对方建议采取后续措施。

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：王英

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158