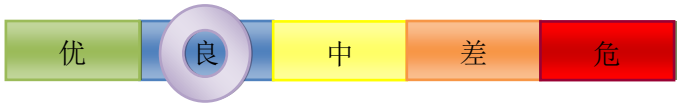
国家互联网应急中心

2017 年第 40 期

9 月 25 日-10 月 1 日

网络安全信息与动态周报

本周网络安全基本态势

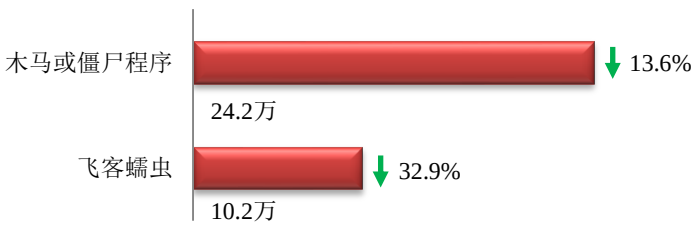


境内感染网络病毒的主机数量	• 34.4万	↓ 20.4%
境内被篡改网站总数 其中政府网站数量	• 1,576 • 29	↓ 12.5% ↓ 48.2%
境内被植入后门网站总数 其中政府网站数量	• 1,095 • 59	↑ 17.2% ↑ 5.4%
针对境内网站的仿冒页面数量	• 282	↑ 5.2%

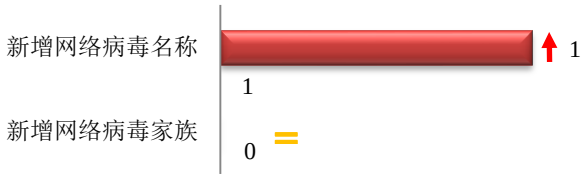
═表示数量与上周相同　↑表示数量较上周环比增加　↓表示数量较上周环比减少

本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 34.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 24.2 万以及境内感染飞客（conficker）蠕虫的主机约 10.2 万。

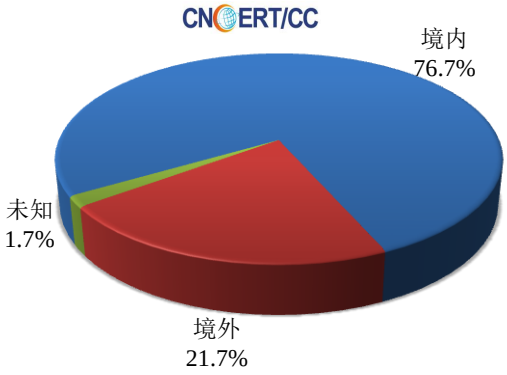


本周 CNCERT 捕获的新增网络病毒文件，按网络病毒名称统计新增 1 个，按网络病毒家族统计无新增。

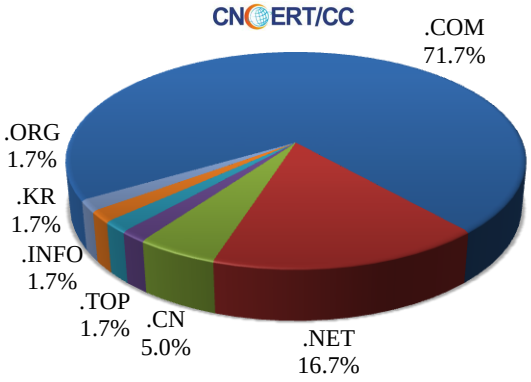


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 60 个，涉及 IP 地址 392 个。在 60 个域名中，有 21.7%为境外注册，且顶级域为.com 的约占 71.7%；在 392 个 IP 中，有约 8.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 4 个 IP。

本周放马站点域名注册所属境内外分布
(9/25-10/1)



本周放马站点域名所属顶级域的分布
(9/25-10/1)



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。

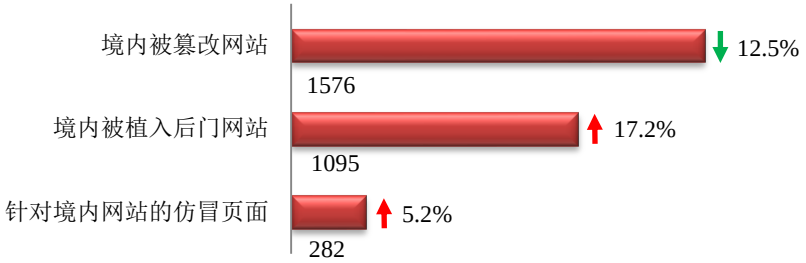
ANVA恶意地址黑名单发布地址

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。

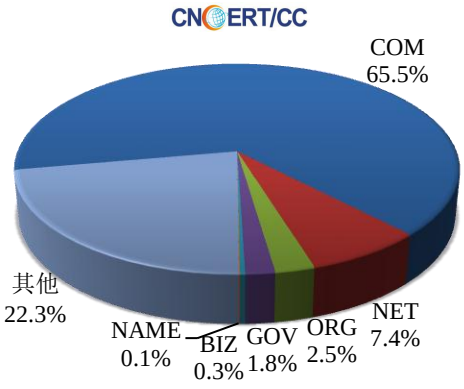
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1576 个；境内被植入后门的网站数量为 1095 个；针对境内网站的仿冒页面数量为 282。

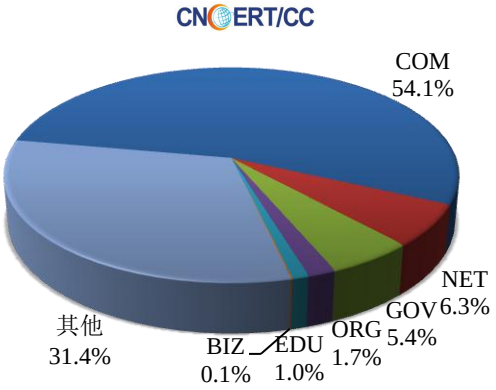


本周境内被篡改政府网站（GOV 类）数量为 29 个（约占境内 1.8%），较上周环比下降了 48.2%；境内被植入后门的政府网站（GOV 类）数量为 59 个（约占境内 5.4%），较上周环比上升了 5.4%；针对境内网站的仿冒页面涉及域名 236 个，IP 地址 109 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被篡改网站按类型分布
(9/25-10/1)



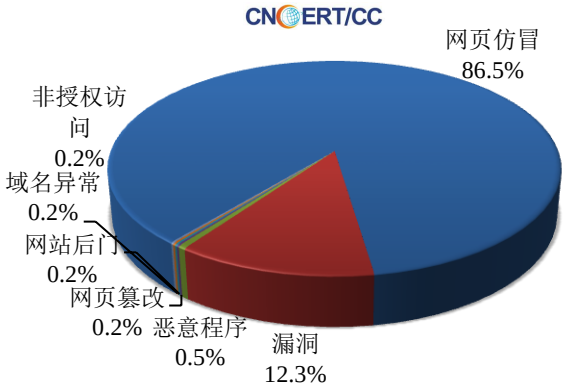
本周我国境内被植入后门网站按类型分布
(9/25-10/1)

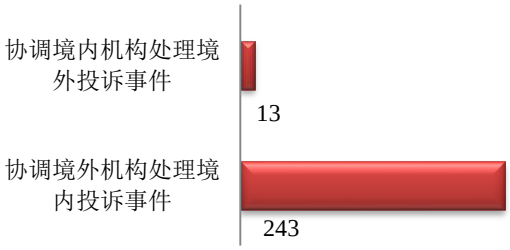


本周事件处理情况

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 600 起，其中跨境网络安全事件 256 起。

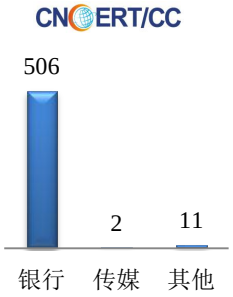
本周CNCERT处理的事件数量按类型分布
(9/25-10/1)



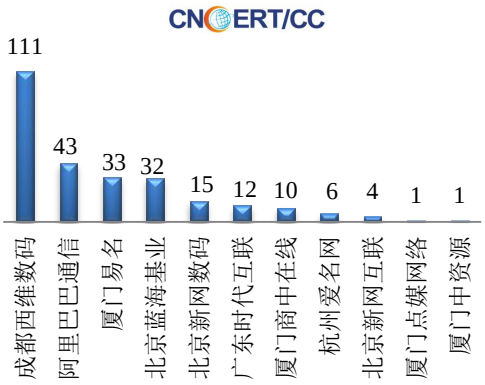


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 519 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 506 起和传媒仿冒事件 2 起。

本周CNCERT处理网页仿冒事件数量
按仿冒对象涉及行业统计(9/25-10/1)

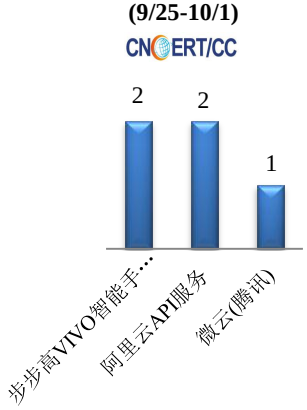


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (9/25-10/1)



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 5 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
(9/25-10/1)



业界新闻速递

1、欧洲网络新规要求及时通知漏洞 否则将重罚

cnBeta.COM9 月 25 日消息 欧洲正准备为企业打造一种新的规则，阻止类似于 equifax 事件的网络安全事件发生，或者发生类似事件时让影响最小化。欧洲新制定的这项规则被称为通用数据保护条例（GDPR），它将在明年 5 月份生效。GDPR 条例规定了公司存储用户数据的方式，并且要求它们在漏洞出现后的 72 小时内通知当局。如果公司不执行，它们将被罚款 4%的全球税收或者 2 千万欧元，两者选取最高额。而拥有欧洲用户信息的所有美国公司也必须遵循这一规定。全球安全公司 RSA 的董事长 Rohit Ghai 称：“这一新规为公司赋予了责任，让其了解它们应当如何管理消费者的数据并且关注用户隐私。”

2、加拿大国家银行因网站故障暴露数百名客户敏感信息

HackerNews.cc9 月 26 日消息 据外媒 9 月 22 日报道，加拿大国家银行于上周发表声明，宣称由于技术原因网站出现故障，导致逾 400 名客户敏感信息在线暴露，其中包括客户姓名、出生日期、电话号码与电子邮件地址等。加拿大国家银行表示，该故障与其网站上的电子表格信息录入相关，即允许客户在线填写表单后建立分支预约，从而查看此前所有数据。然而，由于技术人员设置不当，导致前面客户完成表单填写后，其他客户再次打开网站的表单时可以看到前面客户所填写的所有信息。不过，好在国家银行在接到通知后立即对其进行了处理。目前，银行已通知受影响客户并将为其提供免费信用监控。此外，加拿大国家银行还建议客户警惕任何潜在的身份窃取或网络钓鱼攻击活动。

3、日本一批社媒账号信息泄露 包括 1.5 万个政府电邮

中新网 9 月 25 日消息 据《读卖新闻》网站报道，由于黑客攻击，日本一批社交网站账号及密码发生泄漏，其中包括 14720 个日本政府或独立行政法人所使用的“go.jp”后缀的电子邮箱地址，日本内阁网络安全中心也提醒相关地方县厅加强注意。据推测，有政府工作人员在使用外部网络时，用工作邮箱作为了用户名进行登录。这些“go.jp”后缀邮箱可能会被盗用或是用于恶意攻击，根据规定是不得私用的。据悉，东京一家网络安全公司在进行网络泄露信息调查中发现了这些“go.jp”后缀的邮箱，之后通报了日本内阁网络安全中心。

4、登机系统故障影响了世界各地的航空公司 造成大规模延误

新浪网 9 月 29 日消息 据外媒报道，周四上午登机系统故障影响了世界各地航空公司，致使无数乘客滞留机场。据英国《电讯报》报道，伦敦希思罗机场和盖特威克机场，巴黎戴高乐机场，以及苏黎世机场、墨尔本机场、约翰内斯堡机场、新加坡樟宜机场和华盛顿特区的里根国家机场均受影响。据报道，全球有超过 100 个机场和一些航空公司的网上登机服务遭遇问题。这些问题可追溯到软件供应商 Amadeus 及其 Amadeus Altea 登机软件。在当地时间周四下午 2 点 30 分发表的声明中，该公司表示问题已经解决。虽然软件现在正常运行，但世界各地的机场仍然出现了延误的连锁效应。

5、德勤电邮平台遭遇公司史上最严重黑客攻击，超 500 万封电子邮件和大量客户知识产权恐被泄露

E 安全 9 月 26 日消息 据英国卫报报道，全球四大会计师事务所之一的德勤公司近日爆出公司史上最严重的黑客攻击事件，超过 500 万份内部邮件疑遭泄露，这些邮件中包含了大量德勤客户的敏感信息和知识产权。这是继 Equifax 和美国证券交易委员会 SEC 黑客事件后，本月连续爆出的第三起足以影响全球经济的重大信息安全事故。据报道，黑客攻击的主要目标是德勤的全球电子邮件服务器，通过入侵该服务器的管理员账号（未启用双因子两步认证），黑客成功获取足够权限访问德清 24.4 万员工与客户之间的往来邮件。这些邮件中包含大量的敏感信息，例如账号密码，以及部分邮件附件中的知识产权信息。目前，德勤公司黑客入侵事件的最终审计和调查结果尚未公布，但是德勤黑客攻击导致的数据泄露事件可能会殃及全球范围大量重要机构，例如政府、金融机构和制药公司。

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。截止 2016 年，CNCERT 与 69 个国家和地区的 185 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：雷君

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158