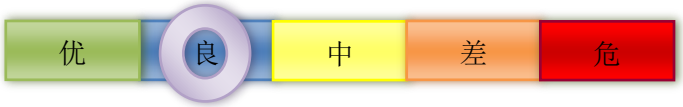
国家互联网应急中心

2017 年第 49 期

11 月 27 日-12 月 3 日

网络安全信息与动态周报

本周网络安全基本态势

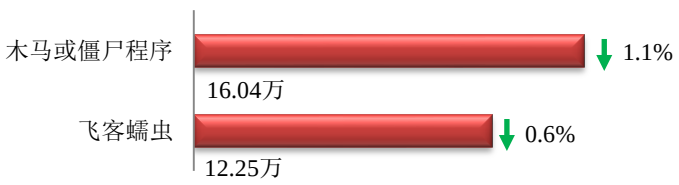


境内感染网络病毒的主机数量	• 28.29万	↓ 0.9%
境内被篡改网站总数 其中政府网站数量	• 1333 • 48	↓ 0.7% ↑ 11.6%
境内被植入后门网站总数 其中政府网站数量	• 982 • 29	↑ 40.5% ↑ 190.0%
针对境内网站的仿冒页面数量	• 369	↑ 0.8%
新增信息安全漏洞数量 其中高危漏洞数量	• 473 • 174	↑ 70.8% ↑ 145.1%

= 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

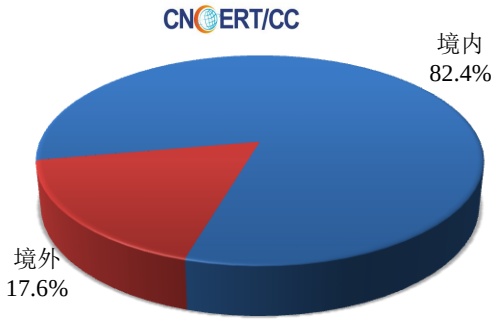
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 28.29 万个，其中包括境内被木马或被僵尸程序控制的主机约 16.04 万以及境内感染飞客（conficker）蠕虫的主机约 12.25 万。

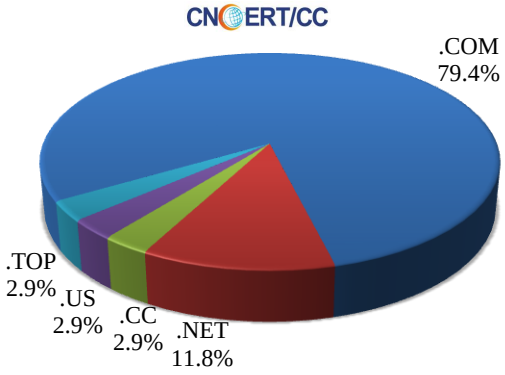


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 34 个，涉及 IP 地址 232 个。在 34 个域名中，有 17.6%为境外注册，且顶级域为.com 的约占 79.4%；在 232 个 IP 中，有约 25.9%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 2 个 IP。

本周放马站点域名注册所属境内外分布
(11/27-12/3)



本周放马站点域名所属顶级域的分布
(11/27-12/3)



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。

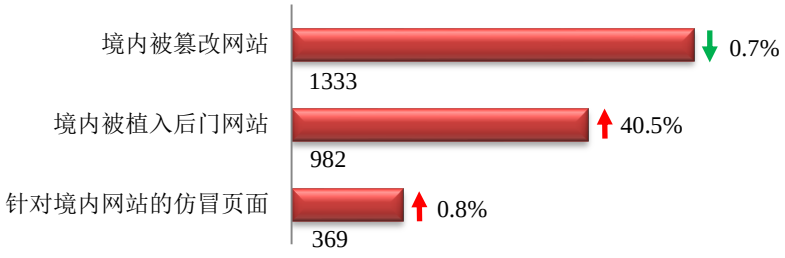
ANVA恶意地址黑名单发布地址

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。

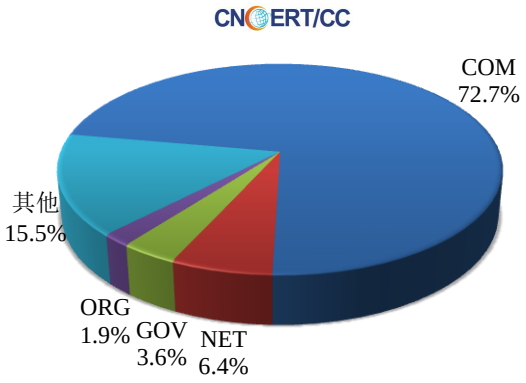
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1333 个；境内被植入后门的网站数量为 982 个；针对境内网站的仿冒页面数量为 369。

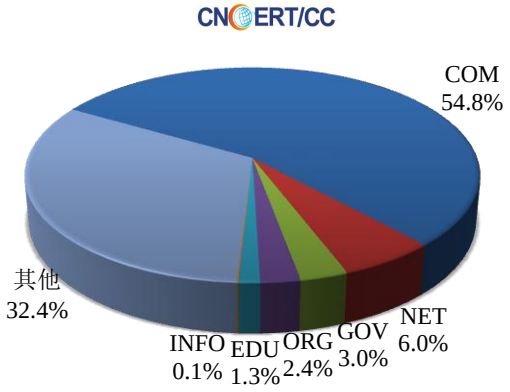


本周境内被篡改政府网站（GOV 类）数量为 48 个（约占境内 3.6%），较上周环比上升了 11.6%；境内被植入后门的政府网站（GOV 类）数量为 29 个（约占境内 3.0%），较上周环比上升了 190.0%；针对境内网站的仿冒页面涉及域名 319 个，IP 地址 146 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被篡改网站按类型分布
(11/27-12/3)

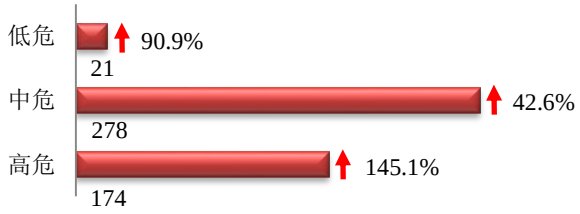


本周我国境内被植入后门网站按类型分布
(11/27-12/3)

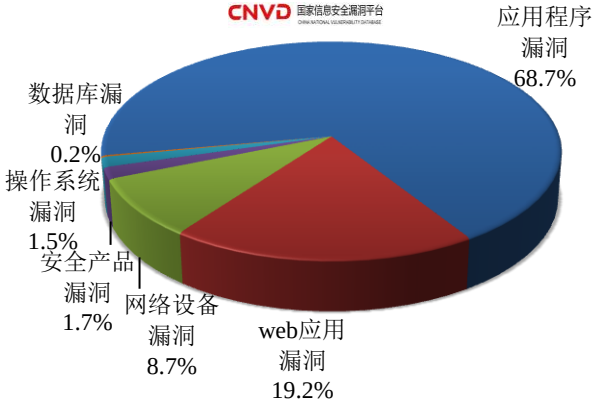


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 473 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
(11/27-12/3)



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。

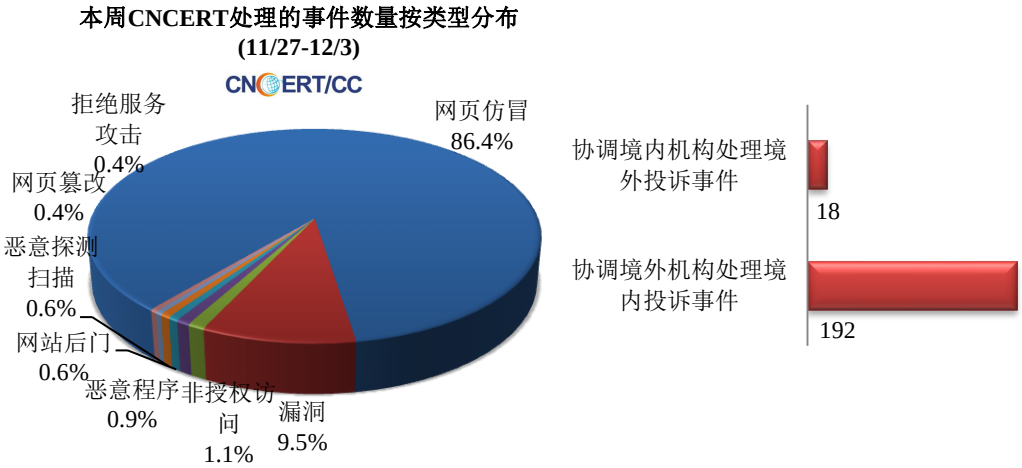
CNVD漏洞周报发布地址

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。

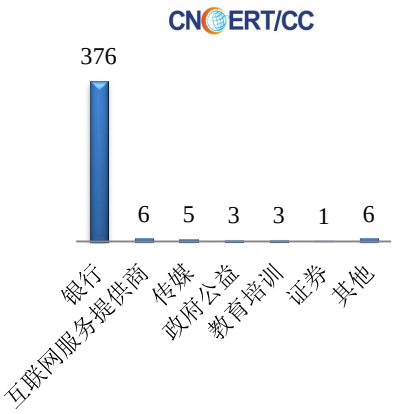
本周事件处理情况

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 463 起，其中跨境网络安全事件 210 起。

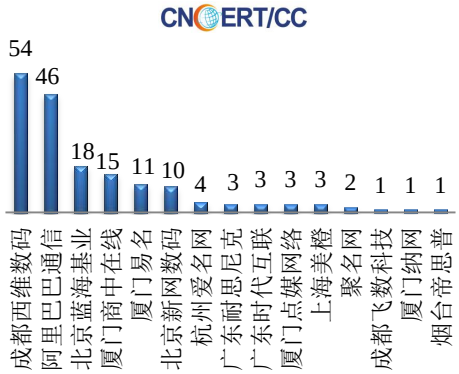


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 400 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 376 起和互联网服务提供商仿冒事件 6 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(11/27-12/3)

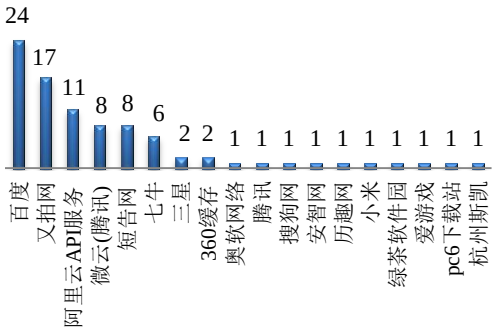


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (11/27-12/3)



本周，CNCERT 协调 18 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 88 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 (11/27-12/3)



业界新闻速递

1、继 WannaCry 勒索软件攻击后，英国 NHS 预将投入 2000 万英镑增强网络防御体系

HackerNews.cc11 月 29 日消息 据外媒 11 月 27 日报道，由于今年 5 月中旬 WannaCry 勒索病毒的肆意爆发，导致英国医疗服务组织（NHS）的 IT 系统出现大规模停滞现象。对此，NHS 经慎重考虑后于近期宣布将投入 2000 万英镑成立一所新安全运营中心，以便帮助各医疗机构免受网络攻击、提高其信息安全领域现有能力（例如：黑客道德行为、漏洞测试和恶意软件分析），以及为当地医疗服务组织提供网络安全咨询和指导。英国医疗服务系统数字安全中心的负责人丹•泰勒（Dan Taylor）表示：“安全运营中心将加强当前数据安全服务、支持卫生和医疗系统、保护敏感患者信息，也将提高目前在黑客道德行为、漏洞测试与恶意软件的取证分析方面以及预测未来漏洞的能力。目前，NHS 正寻找一个合作伙伴来联合运营该安全中心，以便灵活地帮助各医疗组织引入更多专业技能。NHS 的发言人表示:“这可能包括对未来事件的实地或远程支持，对更多需求的保证或输入，从而保证国家系统安全运行”。据悉，新安全中心将设在利兹，但尚未确定具体开放日期。

2、澳大利亚提出消费者新法案，意在促进银行与金融机构数据安全改革

HackerNews.cc11 月 28 日消息 据外媒 ZDNet11 月 26 日报道，澳大利亚政府于近期提出一项新消费者法案，允许公民访问银行、能源、通信以及互联网等交易数据。与此同时，还将同意各企业或政府机构与第三方合作厂商共享数据，以便促进全球网络安全，保护家庭、消费者、企业和政府免遭犯罪攻击。相关人士获悉，该消费者法案一旦通过，其数据权限将由澳大利亚竞争与消费者委员会（ACCC）和澳大利亚信息专员机构（OAIC）联合监管。澳大利亚财政部部长 Scott Morrison 于今年早些时候在悉尼举行的 2017 亚洲未来峰会上表示："开放式银行业务将会改变澳大利亚经济的发展。我们可以做出的最大变化之一就是在未来 20 年内与这个领域最具权威的机构－生产力委员会联合提高澳大利亚公民隐私安全。此外，在能源方面，国家电力市场未来安全的独立审查也需要与其保持一致，并由澳大利亚政府理事会同意，从而提高消费者获取与分享能源数据的能力。同样，在通信方面，该项改革将帮助消费者在其市场上找到最适合他们的策划，并使其实际服务的使用与预算匹配。据悉，澳大利亚政府将于 2018 年提出新联邦立法落实这些改革。

3、美国家信用联盟因亚马逊 AWS S3 配置不当，逾 100GB 用户敏感信息在线暴露

HackerNews.cc12 月 3 日消息 网络安全公司 UpGuard 研究人员 Chris Vickery 于近期发现美国国家信用联盟（NCF）托管的亚马逊 AWS S3 存储器因配置不当，导致逾 100G 用户敏感数据在线暴露，其中包括用户姓名、地址、社保号码、银行账号以及信用报告等具体信息。据称，由美国三大知名信用机构 Equifax、Experian 与 TransUnion 整理的数千份客户信用报告也位于其中。UpGuard 网络分析师 Dan O' sullivan 在博客中写道："经调查发现 NCF 创建的存储库中包含个性化信贷蓝图，即以一种特定形式收集用户大量敏感信息，包括客户所抵押的贷款细节以及信用卡账单支付时间。此外，该存储库中还包含了 NCF 员工访问客户记录，以及屏幕监控程序记录的所有计算机桌面视频。然而不管怎样，所有在线泄露的数据都极有可能遭黑客恶意利用，从而导致客户个人财产被窃。"

4、美国 DHS 24.6 万员工信息泄露

E 安全 12 月 1 日消息 今年 5 月，美国国土安全部（DHS）一名员工的家用电脑服务器被发现存有 24.6 万名 DHS 员工的个人敏感信息，涉及截至 2014 年底进入 DHS 的雇员。DHS 监察长 John Roth（约翰·罗斯）11 月 24 日向国会主要议员发出报告指出，这台服务器还被发现存放着来自案件调查管理系统的 15.9 万个案卷副本，涉及的个人信息包含姓名、社保号和出生日期。所有潜在受影响雇员都将获得 18 个月的信用监控服务。Roth 的代理首席信息安全官 5 月 11 日向 DHS 官员报告了这起数据泄露，相关人员审核了其中细节后，DHS 代理部长 Elaine Duke（伊莱·恩杜克）8 月 21 日决定通知受影响的雇员。DHS 隐私办公室目前正在完善通知受影响雇员的细节，监察长办公室的官与 DHS 紧密合作完成这项工作。相关责任人已被开除。

5、Uber 数据泄露事件涉及 270 万英国用户 或面临巨额罚款

新浪网 11 月 30 日消息 北京时间 11 月 30 日凌晨消息，Uber 对英国数据保护监督机构称，在 2016 年的用户数据泄露事件中，大约有 270 万用户受到影响，这覆盖了大部分英国 Uber 用户。Uber 向英国 Information Commissioner's Office（ICO）称，于上周披露出来的信息泄露事件影响到了约 5700 万全球 Uber 用户，泄露的

内容包括用户的用户名、手机号、和电子邮件地址等。ICO 要求 Uber 尽早通知那些受影响的英国 Uber 司机和用户。Uber 新 CEO 在上周宣称，在 2016 年信息泄露事件发生后并没有及时披露出来。而在现行英国法律中，未及时向监管机构披露信息泄露事实的公司将面临最高 50 万英镑的罚款。

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：郭禹

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158