国家互联网应急中心

网络安全信息与动态周报

2018 年第 9 期

2 月 26 日-3 月 4 日

CNCERT/CC

本周网络安全基本态势

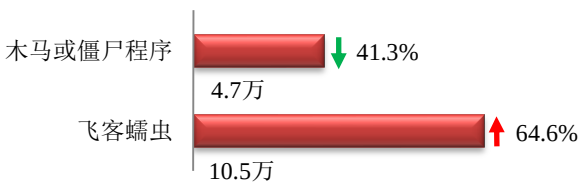
境内感染网络病毒的主机数量	•15.2万	5.3%
境内被篡改网站总数 其中政府网站数量	•1965 •30	9.6% 3.4%
境内被植入后门网站总数 其中政府网站数量	•653 •12	1.2% 200.0%
针对境内网站的仿冒页面数量	•288	213.0%
新增信息安全漏洞数量 其中高危漏洞数量	•397 •144	171.9% 364.5%

Z

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

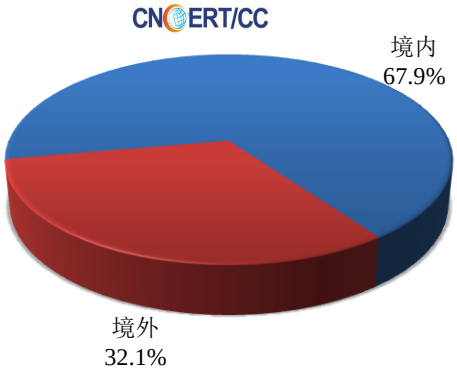
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 15.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 4.7 万以及境内感染飞客（conficker）蠕虫的主机约 10.5 万。

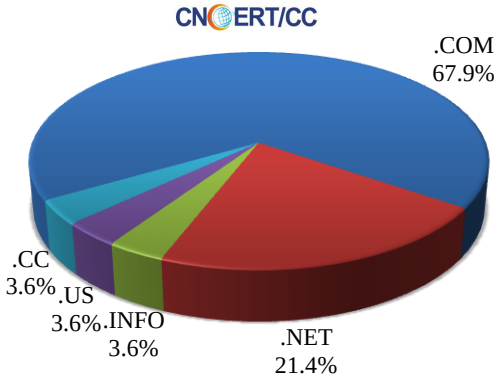


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 28 个，涉及 IP 地址 63 个。在 28 个域名中，有 32.1%为境外注册，且顶级域为.com 的约占 67.9%；在 63 个 IP 中，有约 39.7%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 1 个 IP。

本周放马站点域名注册所属境内外分布
(2/26-3/4)



本周放马站点域名所属顶级域的分布
(2/26-3/4)



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。

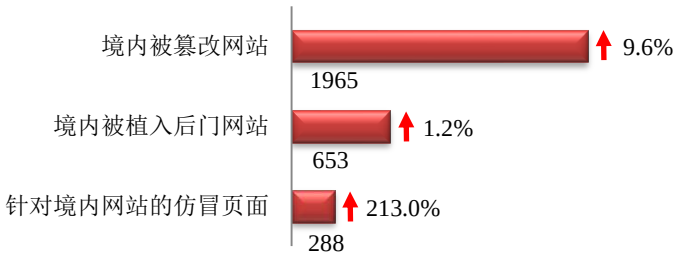
ANVA恶意地址黑名单发布地址

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。

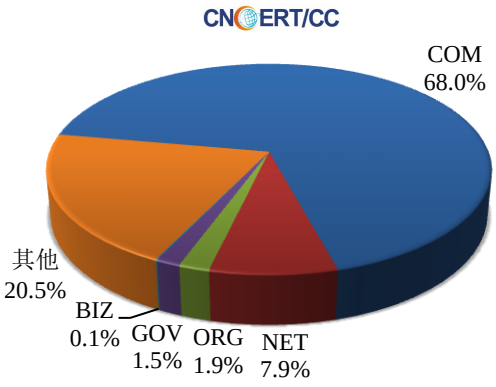
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1965 个；境内被植入后门的网站数量为 653 个；针对境内网站的仿冒页面数量为 288。

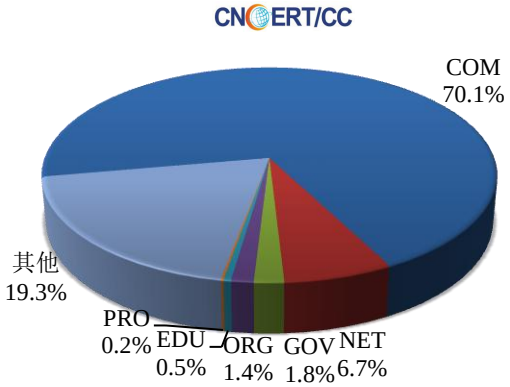


本周境内被篡改政府网站（GOV 类）数量为 30 个（约占境内 1.5%），较上周环比上升了 3.4%；境内被植入后门的政府网站（GOV 类）数量为 12 个（约占境内 1.8%），较上周环比上升了 200.0%；针对境内网站的仿冒页面涉及域名 250 个，IP 地址 97 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被篡改网站按类型分布
(2/26-3/4)

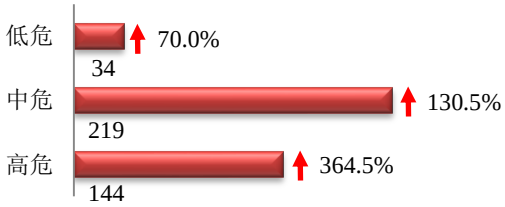


本周我国境内被植入后门网站按类型分布
(2/26-3/4)

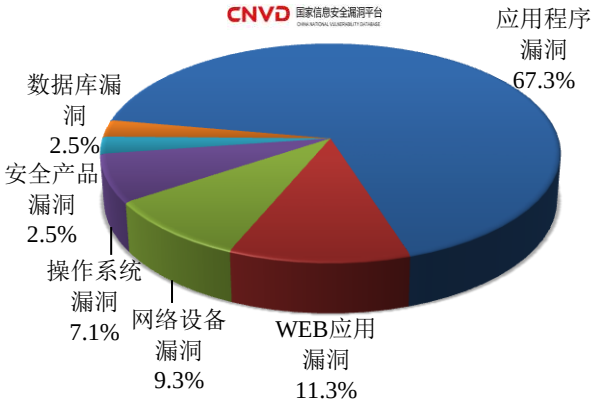


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 397 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
(2/26-3/4)



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

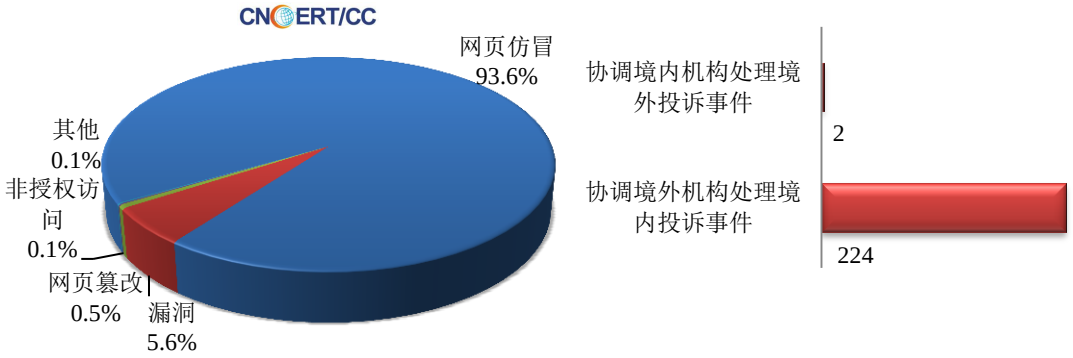
http://www.cnvd.org.cn/webinfo/list?type=4

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

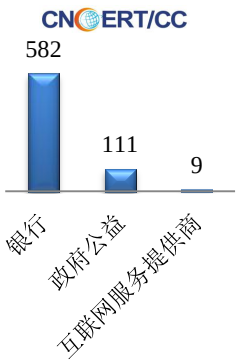
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 750 起，其中跨境网络安全事件 226 起。

本周CNCERT处理的事件数量按类型分布 (2/26-3/4)

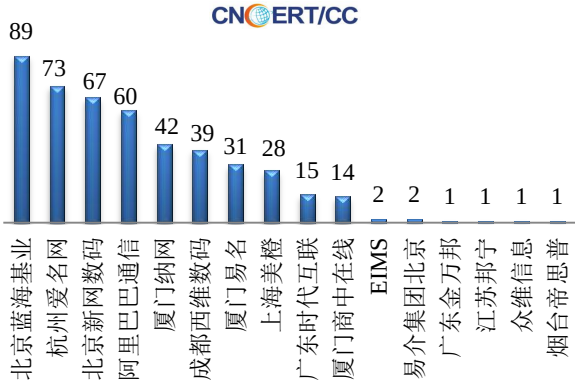


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 702 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 582 起和政府公益仿冒事件 111 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(2/26-3/4)

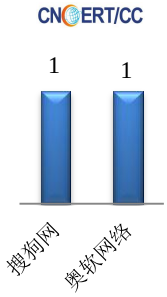


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (2/26-3/4)



本周，CNCERT 协调 2 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 2 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
(2/26-3/4)



业界新闻速递

1、加拿大政府斥资 10 亿美元预算用于打击网络犯罪

HackerNews.cc3 月 2 日消息 外媒 2 月 25 日消息，有关消息人士向新闻媒体透露，加拿大联邦政府预计为网络安全引入 10 亿美元的资金，以解救网络犯罪盛行、政府难以应对的困境。根据加拿大当地媒体报道，加拿大政府将于本周发布预算细节：拟议的预算中将为打击国家网络犯罪提供资金，这可能会包括培训下一代网络专业人员、通过外包本地私营公司来加强军方的网络安全能力的费用。此外，预算还将为政府和私营部门共同开发的网络项目提供资金。例如，加拿大的网络安全由加其信息和技术公司提供，而这些公司将与联邦政府合作开发硬件和软件解决方案。与此同时，一些匿名消息人士告诉加拿大 CBC 新闻 ，鉴于美国 2016 年总统选举期间发生的事情， 加拿大联邦政府可能还打算获得单独资金，以帮助保护 2019 年的全国选举免受外国干涉。

2、美国海军陆战队成员逾 2 万份高度敏感数据泄露

HackerNews.cc3 月 3 日消息 外媒 3 月 1 日消息，美国海军陆战队在本周遭受了重大的数据泄露，超过 21,000 名海军陆战队员、水手以及普通公民的高度敏感信息被意外暴露在未加密的电子邮件中。据悉，邮件附件中列出了被泄露人员的个人财务详细信息，其中包括截短的社会安全号码、信用卡信息、银行路线号码、电子资金转账详情、住宅位置、邮寄地址以及紧急联系信息。据美国海军海军陆战队时报报道，该起事件是由于美国国防部的国防旅行系统（DTS）在 2 月 26 日将一封包含高度敏感个人信息的邮件分发到错误的电子邮件名单中（未分类的“usmc.mil”海军域名以及民用帐户）而造成的。目前具体有多少人接收到了邮件还并不清楚。

3、德国政府称其网络遭遇黑客攻击，未透露袭击者身份

新浪网 3 月 1 日消息 据德国内政部发言人 2 月 28 日的消息，德国政府计算机网络遭遇了黑客攻击，不过目前事件已得到控制。这名发言人在声明中说，受影响的政府机构已采取适当措施保护数据并对此展开调查。

由于相关分析仍在进行中，因此不能透露更多详细信息。据德新社 3 月 1 日报道，德国内政部没有说明黑客的身份。一名内政部的发言人表示：“我们可以证实联邦信息安全局和情报机构正在对一起和政府信息技术及网络有关的安全事件展开调查。”该发言人补充说，遭遇黑客袭击的政府部门已采取必要措施调查袭击和保护其数据资料。目前尚不清楚共有多少数据信息受到影响。

4、美国征信公司信息泄露事件升级 新增 240 万受害者

环球网 3 月 2 日消息 据瑞士资讯 3 月 1 日援引法新社报道，美国征信公司伊奎法克斯（Equifax）当日表示，关于 2017 年 9 月曝出的 1.4 亿用户个人信息泄露事件，近日又发现另外 240 万名受害者。伊奎法克斯的法务调查报告显示，除了有 1.4 亿名美国人姓名、生日和社会安全号码等个人信息泄露外，还有 240 万人用户的个人信息受影响。伊奎法克斯称，之前未发现新的受害客户，是因为他们的社会安全号码并未与部分驾照资讯一同被窃取。而社会安全号码似乎是被黑客攻击的重点。该公司还表示，将会通知这些用户，并为他们提供防盗保护和信用报告监控服务。

5、GitHub 遭受有史以来最严重 DDoS 攻击 现已恢复

cnBeta.COM3 月 2 日消息 北京时间 3 月 1 日凌晨 1 点 15 分，知名代码托管网站 GitHub 遭遇了有史以来最严重的 DDoS 网络攻击，峰值流量达到了 1.35Tbps。尽管此类攻击的特点就是利用如潮水般的流量同时涌入网站，不过本次攻击不同之处在于采用了更先进的放大技术，目的是针对主机服务器产生更严重的影响。这项新技术并非依赖于传统的僵尸网络，而是使用了 memcached 服务器。该服务器的设计初衷是提升内部网络的访问速度，而且应该是不暴露在互联网中的。不过根据 DDoS 防御服务提供商 Akamai 的调查，至少有超过 5 万台此类服务器连接到服务器上，因此非常容易受到攻击。此类服务器没有认证协议，连接到互联网中意味着任何人都可以查询它们。这就是为何在本次攻击中黑客选择使用这些服务器的理由。幸运的是，GitHub 在得到 Akamai 的帮助后，在不到 10 分钟的时间内化解了这次危机。在攻击结束 8 分钟之后，在 Akamai 的介入调查之后，GitHub 证实网站上用户数据的机密性和完整性没有受到影响。

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：张洪

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158