国家互联网应急中心

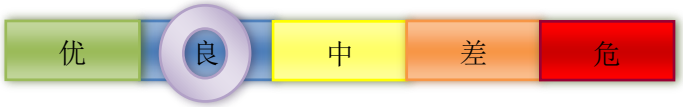
网络安全信息与动态周报

2018 年第 38 期

9 月 17 日-9 月 23 日

CNCERT/CC

本周网络安全基本态势

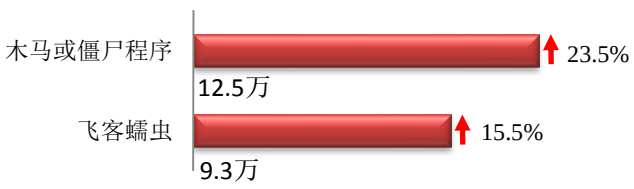


境内感染网络病毒的主机数量	•21.8万	19.8%
境内被篡改网站总数 其中政府网站数量	•504 •38	12.3% 15.2%
境内被植入后门网站总数 其中政府网站数量	•682 •29	8.8% 70.6%
针对境内网站的仿冒页面数量	•2471	14.4%
新增信息安全漏洞数量 其中高危漏洞数量	•375 •109	24.6% 6.8%

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*

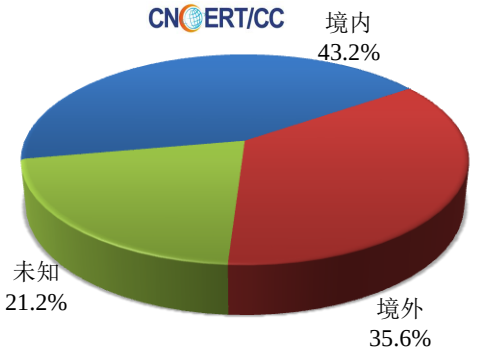
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 21.8 万个，其中包括境内被木马或被僵尸程序控制的主机约 12.5 万以及境内感染飞客（conficker）蠕虫的主机约 9.3 万。

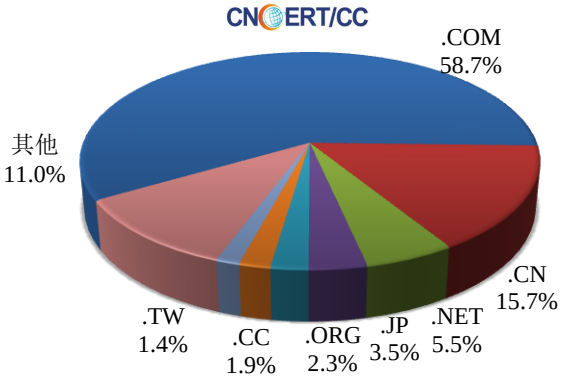


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 3475 个，涉及 IP 地址 83231 个。在 3475 个域名中，有 35.6%为境外注册，且顶级域为.com 的约占 58.7%；在 83231 个 IP 中，有约 26.7%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 485 个 IP。

本周放马站点域名注册所属境内外分布
(9/17-9/23)



本周放马站点域名所属顶级域的分布
(9/17-9/23)



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。

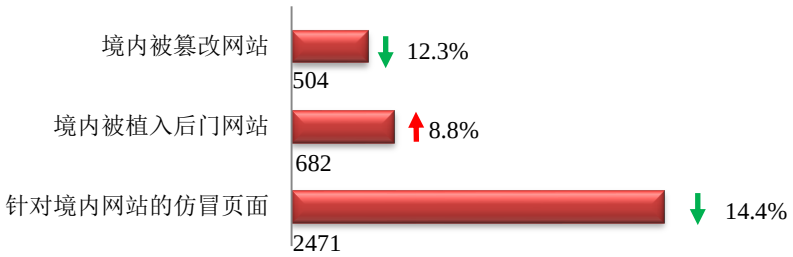
ANVA恶意地址黑名单发布地址

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。

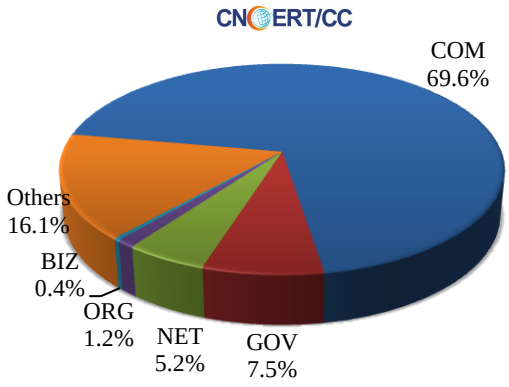
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 504 个；境内被植入后门的网站数量为 682 个；针对境内网站的仿冒页面数量为 2471。

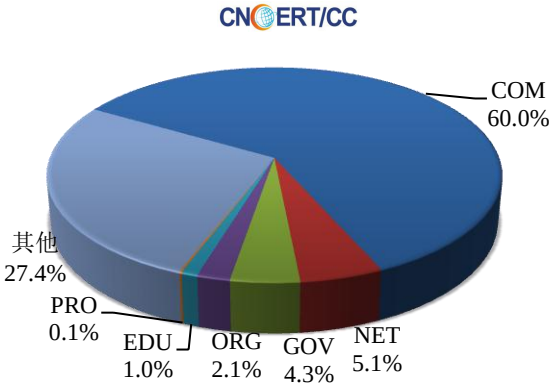


本周境内被篡改政府网站（GOV 类）数量为 38 个（约占境内 7.5%），较上周环比上升了 15.2%；境内被植入后门的政府网站（GOV 类）数量为 29（约占境内 4.3%），较上周环比上升了 70.6%；针对境内网站的仿冒页面涉及域名 911 个，IP 地址 350 个，平均每个 IP 地址承载了约 7 个仿冒页面。

本周我国境内被篡改网站按类型分布
(9/17-9/23)

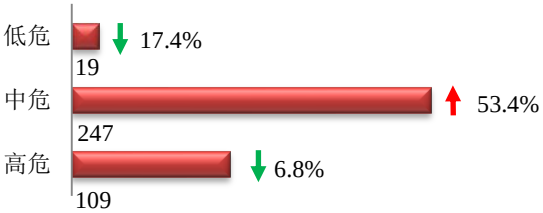


本周我国境内被植入后门网站按类型分布
(9/17-9/23)

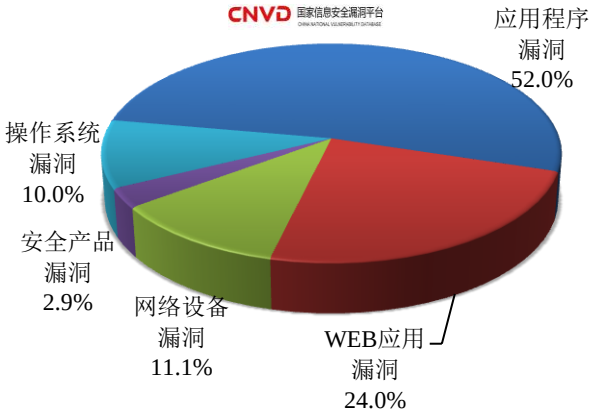


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 375 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
(9/17-9/23)



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

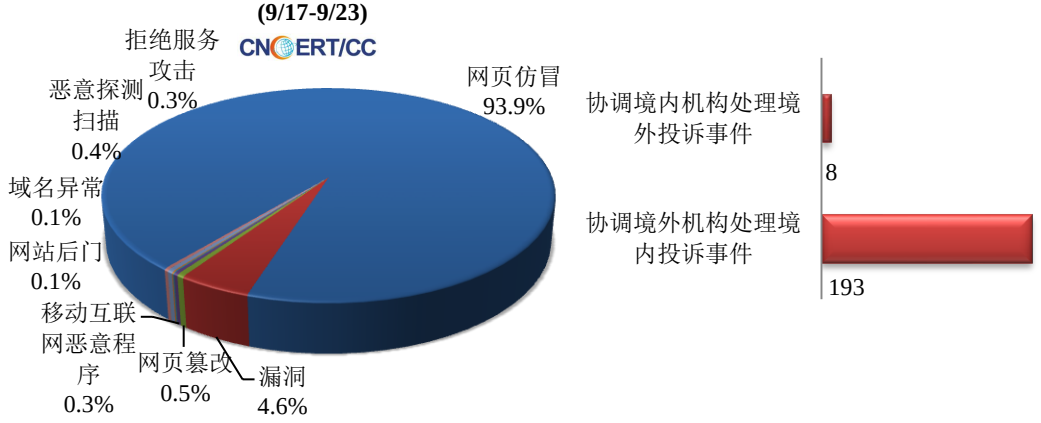
http://www.cnvd.org.cn/webinfo/list?type=4

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

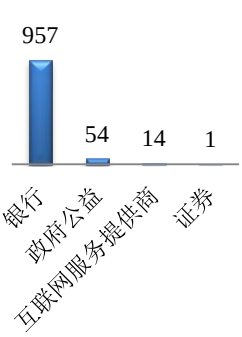
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 1093 起，其中跨境网络安全事件 201 起。

本周CNCERT处理的事件数量按类型分布 (9/17-9/23)

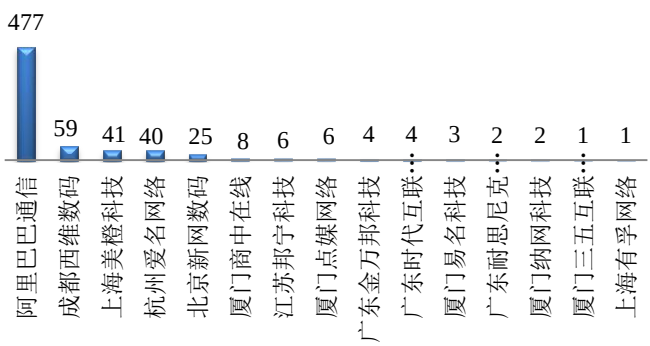


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1026 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 957 起和政府公益仿冒事件 54 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(9/17-9/23)

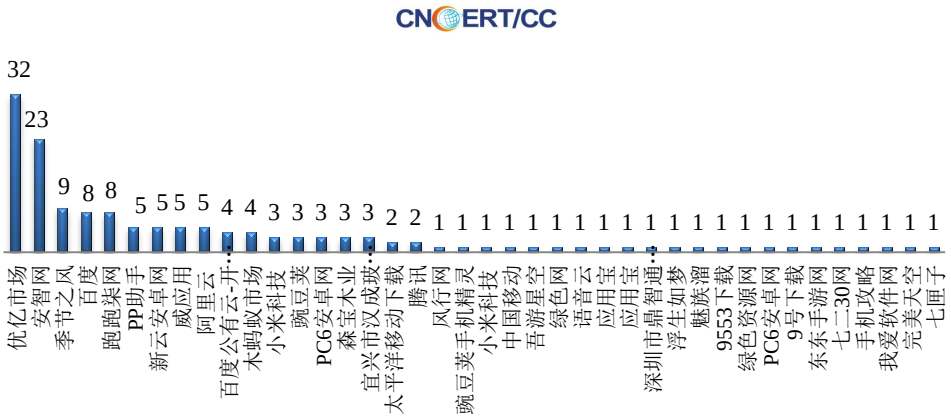


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (9/17-9/23)



本周，CNCERT 协调 40 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 149 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
(9/17-9/23)



业界新闻速递

1、美国特朗普总统签署《国家网络战略》 应对来自网络的威胁

cnBeta.COM9 月 21 日消息 美国总统特朗普的国家安全事务助理约翰·博尔顿 20 日表示，特朗普当天签署了国家网络战略，以加强应对网络威胁。博尔顿在对媒体的吹风会上表示，国家网络战略将指示美国政府采取行动确保长期改善所有美国人的网络安全。

白宫新闻办公室发表声明称，国家网络战略的核心是增强美国网络安全，该战略将有助于保护网络空间成长为经济增长和创新的引擎，同时遏制在网络空间造成不稳定的行为，此外还将保持互联网的长期开放性，支持并加强美国利益。

美国媒体分析称，当天发布的国家网络战略最值得注意的是，美国将采取“进攻性”的行动来制止和应对网络攻击。博尔顿在吹风会上说，对于任何正在对美国采取网络行动的国家来说，他们应该意识到，我们将同时从进攻和防守两个方面进行回应。

2、新加坡将设立东盟-新加坡网络安全卓越中心

E 安全 9 月 19 日讯 新加坡副总理张志贤（Teo Chee Hean）9 月 18 日在第三届新加坡国际网络活动周的开幕上宣布，新加坡将设立东盟-新加坡网络安全卓越中心，以加强东盟成员国的网络战略制定、立法和研究能力。该中心将扩大现有的东盟网络能力计划，并培训东盟地区的国家计算机应急响应小组（CERT），并促进 CERT 与 CERT 之间进行信息开源共享。3、美国 NIST 联合 DHS 发布第一份防范 BGP 劫持的安全标准草案

3、尼日利亚网络安全专家协会呼吁总统签署电子交易法案

E 安全 9 月 18 日讯 据报道，尼日利亚网络安全专家协会（简称 CSEAN）呼吁该国总统布哈里（Muhammadu Buhari）签署电子交易法案，这项法案认可电子合同的有效性，其关乎证据、在线交易安全、电子签名、信息披露、个人数据保护和消费者权利保护。CSEAN 主席 Remi Afon 表示，该法案将保护尼日利亚人的金融交易，并会保护银行及基础设施。

4、谷歌警告：美国参议员 Gmail 账号已成为国外黑客攻击目标

cnBeta.COM9 月 21 日消息谷歌证实，部分美国参议员和助手的 Gmail 账号已成为国外政府黑客重点针对的目标。但谷歌的发言人拒绝透露更多的细节，包括有多少人受到影响，这些有国家支持的攻击都来自哪里，以及何时发布警告等等。

本周三来自来自俄勒冈州的民主党参议员罗恩·怀登（Ron Wyden）致信参议院领导机构，称存在电子邮件攻击情况，但只是提及谷歌是“主要科技公司”。谷歌在本周四对外承认。

在 2016 年美国大选中浮出水面的假新闻案件，让谷歌、脸书和推特在内的诸多科技公司焦头烂额。为此在今年的中期选举中这些科技巨头都采取了相应的措施来杜绝此类事件再次发生。

5、比特币软件被曝 DoS 漏洞：开发者紧急修补

新浪科技讯 北京时间 9 月 20 日午间消息，比特币软件被曝存在一个严重漏洞，导致开发者周二紧急商讨，并发布修复方案。

这个漏洞是一个 DoS 漏洞，修复方案已经通过 Bitcoin Core 0.16.3 发出。如果这个漏洞被黑客利用，就有可能去掉节点，最糟糕的情况甚至会导致相当一部分网络暂时崩溃。

但并非所有人都有能力利用这个漏洞。只有矿机可以通过加倍投入交易并将其注入到区块中才能实现。

然而，即便真要尝试这种攻击方式，矿机也会丢失区块奖励，按照目前的价格计算，大约相当于 7.5 万美元。

这个漏洞出现在 Bitcoin Core 0.14.0 中，该软件 2071 年 3 月首次推出，但直到两天前才被发现。正因如此，开发者才紧急采取行动，并在 24 小时内推出解决方案。

幸运的是，多数比特币持有人目前都不必采取任何措施。开发者强调称，“存储的”比特币没有风险。但却会影响到那些使用 Lightning 网络的比特币，这是一种正在开发的交易层，目的是加快交易速度、降低交易成本。

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：顾笑南

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158