国家互联网应急中心

2018 年第 40 期

10 月 1 日-10 月 7 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 | • 16.1万 | ↓ 24.4% |
| 境内被篡改网站总数<br>其中政府网站数量 | • 413<br>• 26 | ↑ 8.1%<br>↓ 13.3% |
| 境内被植入后门网站总数<br>其中政府网站数量 | • 453<br>• 8 | ↓ 26.8%<br>↓ 33.3% |
| 针对境内网站的仿冒页面数量 | • 1318 | ↓ 13.3% |

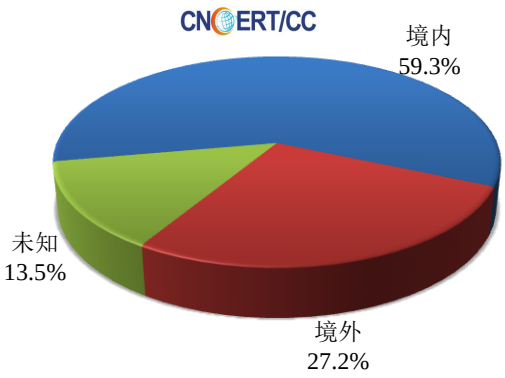
*= 表示数量与上周相同　↑ 表示数量较上周环比增加　↓ 表示数量较上周环比减少*

## 本周网络病毒活动情况

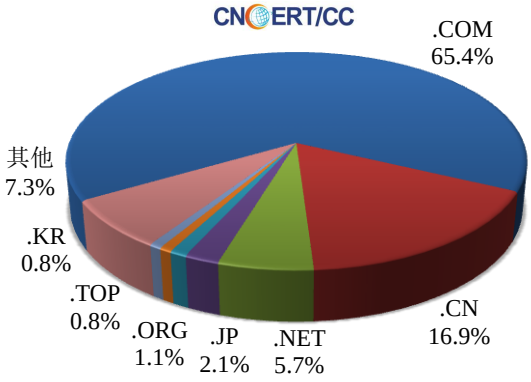
本周境内感染网络病毒的主机数量约为 16.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 9.0 万以及境内感染飞客（conficker）蠕虫的主机约 7.1 万。

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 661 个，涉及 IP 地址 23718 个。在 661 个域名中，有 27.2%为境外注册，且顶级域为.com 的约占 65.4%；在 23718 个 IP 中，有约 36.4%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 81 个 IP。

**本周放马站点域名注册所属境内外分布**
**(10/1-10/7)**




**本周放马站点域名所属顶级域的分布**
**(10/1-10/7)**




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。

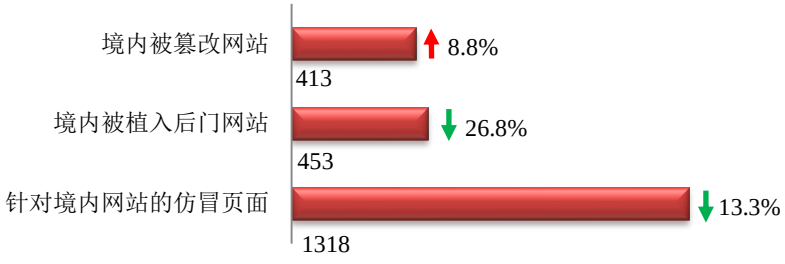
**ANVA恶意地址黑名单发布地址**

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。*

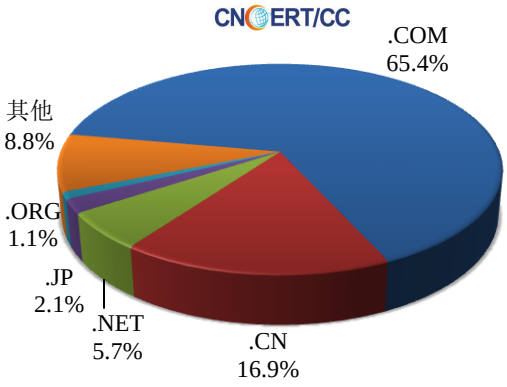
## 本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 413 个；境内被植入后门的网站数量为 453 个；针对境内网站的仿冒页面数量为 1318。

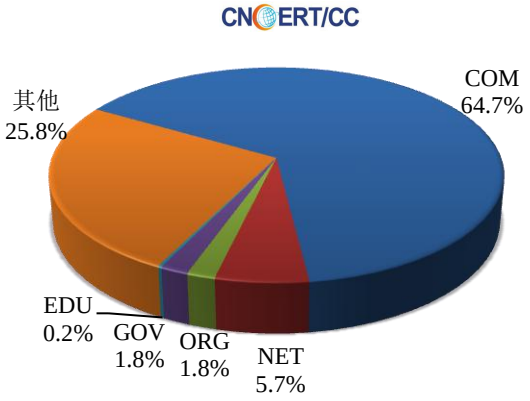


本周境内被篡改政府网站（GOV 类）数量为 26 个（约占境内 6.3%），较上周环比下降了 13.3%；境内被植入后门的政府网站（GOV 类）数量为 8 个（约占境内 1.8%），较上周环比下降了 33.3%；针对境内网站的仿冒页面涉及域名 461 个，IP 地址 213 个，平均每个 IP 地址承载了约 6 个仿冒页面。

**本周我国境内被篡改网站按类型分布**
**(10/1-10/7)**



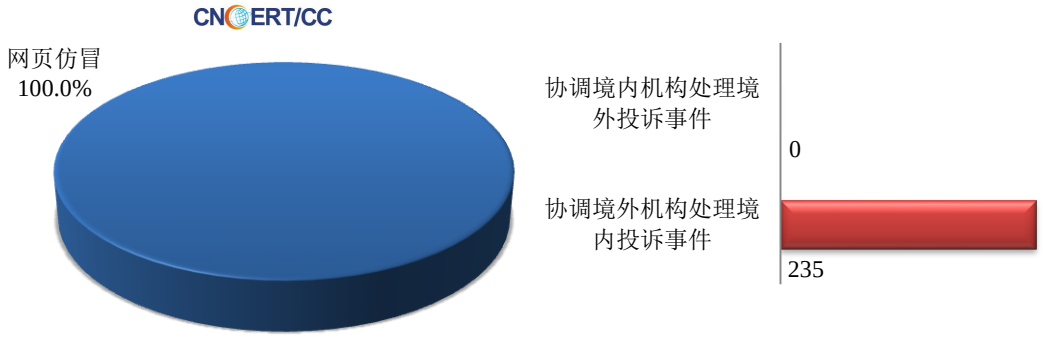

**本周我国境内被植入后门网站按类型分布**
**(10/1-10/7)**




## 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 491 起，其中跨境网络安全事件 235 起。

**本周CNCERT处理的事件数量按类型分布**
**(10/1-10/7)**




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 491 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 491 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(10/1-10/7)


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 (10/1-10/7)


## 业界新闻速递

### 1.白宫发布《国家网络战略》，将“以暴制暴”

E 安全 10 月 6 日消息 白宫方面发布了《国家网络战略》（以下简称“战略”），提出了一系列用于保护美国关键基础设施免受全球网络威胁的具体方法。

该“战略”的建立以美国此前发布的第 13800 号行政令“加强联邦网络与关键基础设施网络安全”、《国家安全战略》内相关网络要素、美国国土安全部（DHS）与商务部发布的僵尸网络报告中的调查结果及建议为基础。

在 2018 年 10 月美国网络安全意识月开始之前，该“战略”的发布标志着美国网络漏洞的修复与网络能力构建工作已经重新受到关注。

此项“战略”概述了一种总体性的“政府范围内”方法，用以指导各机构履行自身网络安全职责与职能。

另外，此项“战略”还标志着政府当局对私营部门，特别是各政府承包商与关键基础设施供应商提出了优先事项与责任分配，并将为其提供设备与服务供应生态系统。与行业建立起合作伙伴关系以实现报告目标成为本项“战略”中的一大核心主题，其既表明了参与机会，也强调了私营部门需要承担的责任。

此外，虽然此项“战略”本身没有特别提及攻击性网络行动，但其中强调政府应采取更具攻击性的姿态，从而充分运用“国家权力工具……以预防、应对并阻止针对美国的恶意网络活动。”

此项战略立足于四大关键性支柱：

保护政府网络与关键基础设施；

发展创新与网络人力；

通过提高美国归因能力以阻止恶意网络活动；

向国外输出开放及自由的互联网价值主张。

支柱一：保护美国民众、国土以及美国人的生活方式

此项支柱的目标在于通过提高弹性与网络风险管理能力以保护美国公共及私有信息网络。

这份报告呼吁“美国政府、私营企业以及每一位民众都应采取立即且果断的行动以加强网络安全，各方都应努力确保网络处于其控制之下并相互支持。”

这方面的优先事项包括以集中方式管理并监督联邦机构网络安全、调整风险管理与信息技术，同时改善联邦供应链风险管理以遵循行业最佳实践。

供应链风险管理

此项“战略”指出，联邦政府“将把供应链风险管理纳入机构采购与风险管理流程”，从而严格审查及评估承包商风险管理实践，并利用联邦政府的购买力鼓励私营部门采用网络安全最佳实践与标准。

关键基础设施保护

此支柱的关键部分，在于强调对关键基础设施的保护。政府当局将优先考虑七大关键性风险缓解领域，具体包括国家安全、能源与电力、银行与金融、健康与安全、通信、信息技术以及运输。

信息与通信技术供应商

此次“战略”亦强调了信息与通信技术（简称 ICT）供应商的重要性，特别是考虑到其提供的跨部门支持功能。美国政府当局承诺加强与信息通信技术供应商间的信息共享能力，包括与经过审查的信息通信技术运营商共享机密威胁与漏洞信息。

另外，此项“战略”还将通过改进事件报告以打击网络犯罪。具体举措包括与私营企业合作以应对匿名化及加密等技术带来的挑战，从而获取时间敏感性信息。

支柱二：促进美国繁荣

第二大支柱旨在通过“将网络空间发展为经济增长、创新与效率的开放驱动引擎”以保护美国在技术生态系统中的影响力。

在这方面，政府计划通过鼓励与引导建立起极具适应能力的安全技术市场，确保其优先考虑创新并投资下一代基础设施，从而保持美国在新兴技术领域的领导地位，同时促进全生命周期网络安全水平。

联邦政府当局计划消除信息共享层面的政策性障碍，并将与国际同行合作以推动全球范围内以行业为导向、以风险为基础的现有网络安全实现方法。

这一支柱的另一部分内容，则要求通过保持强大而平均的知识产权保护制度与美国发展路线机密性及完整性以保护美国的才智成果。

此项“战略”还强调建立并维持人才管道，通过员工再培训、扩大教育机会以及加强联邦网络安全工作人员水平来发展出强大的网络安全工作队伍。

支柱三：以力量为基础保持和平

此项支柱强调一种更具前瞻性的姿态，旨在促进建立“网络空间中负责任的国家行为框架”，并通过针对恶意活动实施“迅速、高成本且透明的制裁性措施”作为综合性战略，从而加强针对美国及其合作伙伴的恶意网络活动的归因与制止性努力。

白宫发布《国家网络战略》，将“以暴制暴”-E 安全

其中将侧重于建立领先、客观的协作性情报收集工作，从而实现对网络空间内恶意行为的归因与阻止。

报告当中提到一项新的具体举措，即制定网络威慑倡议，其中要求“美国与各志同道合的国家开展合作、协调与支持，共同建立起对重大恶意网络事件的响应机制，具体包括建立情报共享渠道、支持归因声明、支持回应行动的公开声明以及共同对恶意活动方施加制裁。”

支柱四：提升美国影响力

此项“战略”的最后一项支柱，旨在保护互联网的长期开放性与互操作性，优化大师促进美国利益。

美国政府将继续与各志同道合的国家、行业以及民间社会开展合作，在全球范围内推进人权与互联网自由思维的建设。其还将应用基于良好技术原则的行业领导标准，推广可互操作且可靠的通信基础设施与互联网连接，同时致力于在全球范围内建立网络能力。

**2.俄罗斯遭美英澳等国“围攻”：指认其发起网络攻击**

新华网 10 月 6 日讯 美国司法部发布 7 人的姓名，他们的年龄 27 岁至 46 岁，所受到的罪名指控包括电脑入侵、电信欺诈、身份盗窃和洗钱。

按照美国司法部的说法，2014 年 12 月至 2018 年 5 月，被告利用“黑客”手段传播数百名反兴奋剂官员和运动员的个人信息；利用“钓鱼”电子邮件盗取西屋电气员工信息，以入侵这家企业的网络；窃取个人和实体的计算机文件，用于干扰 2016 年美国总统选举。

美方认定，俄方通常发起远程网络攻击，不成功的情况下会在目标所在地发起“现场”或“近距离”攻击；俄军情报总局官员经常携带先进设备，前往全球各地，利用无线网络发起攻击。

4 日早些时候，英国外交大臣杰里米·亨特说，英国国家网络安全中心认定，俄军情报总局是多起网络攻击的“黑手”。

按照英方说法，俄方攻击对象包括政治、商业、媒体和体育机构，如 2016 年美国总统选举期间入侵民主党全国委员会电脑网络、2017 年入侵世界反兴奋剂机构电脑网络和攻击乌克兰政府部门网络。

澳大利亚政府随后发表声明，呼应英方的说法。

几小时后，荷兰国防部召开记者会，说荷兰安全机构今年 4 月阻止俄罗斯特工对禁止化学武器组织发起网络攻击。位于荷兰海牙的禁化武组织正在调查俄罗斯前特工谢尔盖·斯克里帕尔在英国“中毒”一事。

荷方发布一些照片，称俄罗斯特工在一辆车上装载用于入侵无线网络的设备，停在禁化武组织所在建筑附近。按照荷方的说法，那些俄罗斯人持外交护照，荷方因而驱逐、而非逮捕他们。

加拿大方面 4 日认定，加方已经成为俄方网络攻击的目标，总部位于蒙特利尔的世界反兴奋剂组织遭网络攻击是例证之一。

针对荷方记者会，俄罗斯外交部在一份声明中回应：“西方的间谍妄想症变得越来越严重。”

一名俄方外交部消息人士告诉俄罗斯卫星通讯社记者，俄罗斯没有、也不可能发起西方所说那类攻击，因为禁化武组织的所有机构都有俄方参与。

“我们为什么要盗取信息？我们有接触信息的渠道，所有网络对我们都开放。这是又一次胡说八道。”

针对美方指认，俄外交部副部长谢尔盖·里亚布科夫说，看到美方官员继续用毫无根据的指控破坏俄美关系的氛围，俄方感到遗憾。

里亚布科夫说：“西方再一次受到俄罗斯黑客威胁，这一次号称是入侵几乎全球的网络。”

他警告，俄罗斯已经习惯美方类似做法，但刻意在核大国之间以及国际舞台上制造紧张“是一条危险的路”。

**3.Instagram 被曝拟将用户位置历史数据移交给 Facebook**

新浪科技 10 月 5 日讯 鉴于 Instagram 创始人已经辞职，转移位置历史数据的消息无疑将加剧大众对于 Facebook 进一步利用 Instagram 的担忧。有人发现 Instagram 正在设计一项隐私设置，这将允许其与 Facebook

共享用户的位置历史数据。这就意味着即便你没有在使用 Facebook，Instagram 收集的准确 GPS 坐标也会帮助 Facebook 投放广告并推荐相关内容。令人担忧的一点在于，位置历史分享的设置在设计原型中是默认开启的。用户在其 Facebook 活动日志可以看到这些标志地理位置的数据，其中包括你每天去过地方的地图。

这种数据整合会让那些希望限制 Facebook 监视其生活的用户感到不安。当 Facebook 任命马克·扎克伯格（Mark Zuckerberg）的密友、前 News Feed 高级副总裁亚当·莫塞利（Adam Mosseri）接任 Instagram 总裁一职之后，一些评论家就担心 Facebook 会试图从 Instagram 榨取更多价值。这就包括通过垃圾邮件通知为其主要应用拉动推荐流量、插入额外的广告或是提取更多数据。Facebook 先前已经因为违反对欧洲监管机构的承诺一事被起诉，公司原本承诺不会整合 WhatsApp 与 Facebook 的数据，最终导致 1.22 亿美元的罚款。

Facebook 发言人在 TechCrunch 的采访中表示，“有一点要确认清楚，我们尚未更新位置设置。如你所知，我们经常会基于想法进行一些研发，随着时间的推移，这些想法也许会进一步发展抑或是最终不会进行测试或推出。Instagram 目前没有存储历史数据，如果未来的位置设置出现任何变化，我们都会告诉大家”。这些话证实了一点，Instagram 已经设计了位置历史数据共享的原型，并且正在考虑是否要推出（只不过目前尚未推出）。

提供 Instagram 用户去过哪里的准确位置数据可以帮助 Facebook 通过多个应用程序投放本地广告。如果公司获悉用户去到了一些企业、国家、社区或学校，Facebook 就可以利用这些数据推断他们想要购买的产品并进行推广。它甚至可以显示出用户所在地附近的餐厅或商店广告。就在昨天，TechCrunch 曾报道 Facebook 重新设计了 Nearby Friends 功能，朋友位置信息不再以列表形式显现，而是以地图。从 Instagram 提取位置历史数据可以帮助 Facebook 更新附近的朋友位置地图。

知情人士透露，由于扎克伯格逐渐减少 Instagram 的自主权，双方之间关系愈加紧张，随后 Instagram 创始人凯文·斯特罗姆（（Kevin Systrom）和迈克·克雷格（Mike Krieger）离开了公司。关于 Instagram 应当如何促进 Facebook 取得成功一事，斯特罗姆显然与扎克伯格发生了冲突，尤其是年轻的用户不再使用以前的社交网络，转而使用更新颖的视觉媒体应用。尽管 News Feed 广告库存已经用完且用户开始采用广告商依然在适应的 Stories，Facebook 依然面临营收增长的压力。Facebook 与谷歌正在进行激烈的广告竞争，并将竭尽所能利用好自己的一切优势。

**4. 法律禁止默认密码“admin"，“无意入侵”没那么容易了**

cnBeta.COM10 月 7 日消息 据 techcrunch 报导，加州通过了一项法律，2020 年之后禁止在所有新的消费电子产品中使用“admin”、“123456”和经典的“password”这样的默认密码。

从路由器到智能家居技术在该州建造的每个新设备都必须具有开箱即用的“合理”安全功能，法律特别要求每个设备都带有“每个设备独有的”预编程密码。它还要求任何新设备“包含一个安全功能，要求用户在首次授予设备访问权限之前生成新的身份验证方法”，在第一次打开是强制用户将其唯一密码更改为新的密码。

弱密码问题一直是黑客进行攻击利用的有效且低成本手段，多年来，僵尸网络利用了安全性较差的连接设备的强大功能，在网站上拥有大量的互联网流量，也就是所谓的分布式拒绝服务（DDoS）攻击。僵尸网络通常依赖于默认密码，这些密码在构建时被硬编码到设备中，用户以后不会对其进行更改。

恶意软件使用公开的默认密码侵入设备，劫持设备并诱使设备在用户不知情的情况下进行网络攻击。两年前，臭名昭着的 Mirai 僵尸网络将成千上万的设备拖到了目标 Dyn，这是一家为主要网站提供域名服务的网络公司。通过使 Dyn 无法正常解析域名，导致其它依赖其服务的网站也无法访问，造成在大面积的网络瘫痪。

简单的 Mirai 能够造成大损失的很大原因就在于利用了设备默认的简单密码。

虽然新法可以防止这类僵尸网络，但却无法解决更广泛的安全问题，比如有些攻击是不需要猜测密码的，另一方面，该法律并未要求设备制造商在发现错误时更新其软件，像亚马逊、苹果和谷歌这样的大型设备制造商确实会更新他们的软件，但更多鲜为人知的品牌却不会这样做。

### 5. Facebook 确认：黑客未利用用户登录信息入侵其他网站

cnBeta.COM10 月 3 日消息 Facebook 周二表示，调查人员已确定，在上周披露的大规模网络攻击中，黑客没有利用 Facebook 登录信息去入侵其他网站。Facebook 安全事务副总裁盖伊·罗森（Guy Rosen）在声明中说：“在已确定的攻击发生时，我们分析了第三方服务的访问情况。没有任何证据表明，攻击者使用 Facebook 登录信息访问任何应用。”

Facebook 上周披露了有史以来最严重的一起安全事故。Facebook 表示，黑客窃取了登录代码，从而可以访问近 5000 万个 Facebook 帐号。

本周二，Facebook 股价连续第三天下跌，跌幅 1.9%，至 159.33 美元。

罗森在周五的电话会议上警告称，黑客也可能利用这些信息入侵了第三方网站和应用。用户可以在这些网站和应用上使用 Facebook 信息来登录。

包括一名 Facebook 前高管在内，多名安全专家表示，就今年 5 月底生效的欧盟隐私保护新规而言，Facebook 上周五披露的这起攻击事件可能代表了一种最糟糕的情况。

欧盟的“通用数据保护条例”（GDPR）规定，如果企业未能在数据泄露事件发生的 72 小时内进行披露，那么将面临严厉处罚。安全专家表示，这个时间窗口很紧，调查人员没有足够的时间来确定数据泄露的影响。

Facebook 前首席信息官埃里克斯·斯塔莫斯（Alex Stamos）在 Twitter 上表示：“GDPR 的 72 小时要求带来了有趣影响：在调查完成前，企业就公布了数据泄露事故。”

其结果是，“每个人都对实际影响感到困惑，产生了许多谣言”。他在 Twitter 上说，“一个月后，真相才会被包括在官方文件内。”

伊利诺伊大学芝加哥分校的研究人员估计，有超过 4.2 万家网站使用 Facebook Login 登录服务。因此，Facebook 最初的说法，即黑客可能利用这些信息入侵外部网站，令人震惊。

Facebook 的警告已经促使部分网站启动调查。总部位于英国的旅行网站天巡和宜家旗下的 TaskRabbit 表示，正在调查这起事件对客户的可能影响。Uber 则表示，在调查期间已经关闭了使用 Facebook 登录服务的活跃会话。

## 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：郭禹

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158