国家互联网应急中心

网络安全信息与动态周报

2017 年第 43 期

10 月 16 日-10 月 22 日

CNCERT/CC

本周网络安全基本态势

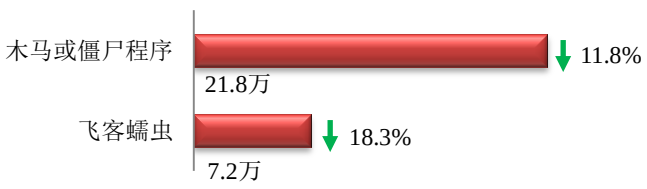
境内感染网络病毒的主机数量	•29.0万	13.5%
境内被篡改网站总数 其中政府网站数量	•1606 •44	41.8% 31.3%
境内被植入后门网站总数 其中政府网站数量	•562 •32	34.1% 23.8%
针对境内网站的仿冒页面数量	•325	2.4%
新增信息安全漏洞数量 其中高危漏洞数量	•597 •114	172.6% 29.5%

v

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

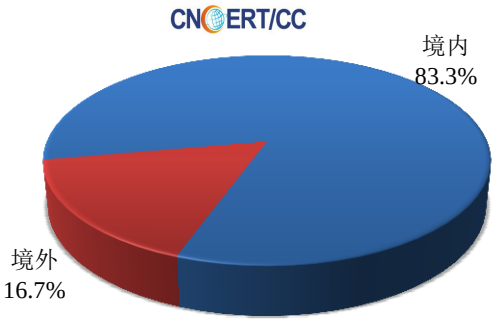
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 29.0 万个，其中包括境内被木马或被僵尸程序控制的主机约 21.8 万以及境内感染飞客（conficker）蠕虫的主机约 7.2 万。

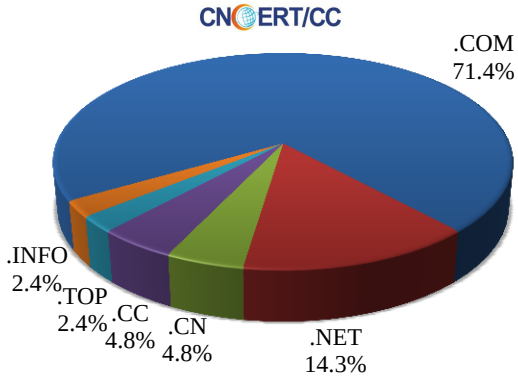


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 42 个，涉及 IP 地址 311 个。在 42 个域名中，有 16.7%为境外注册，且顶级域为.com 的约占 71.4%；在 311 个 IP 中，有约 17.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 4 个 IP。

本周放马站点域名注册所属境内外分布
(10/16-10/22)



本周放马站点域名所属顶级域的分布
(10/16-10/22)



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。

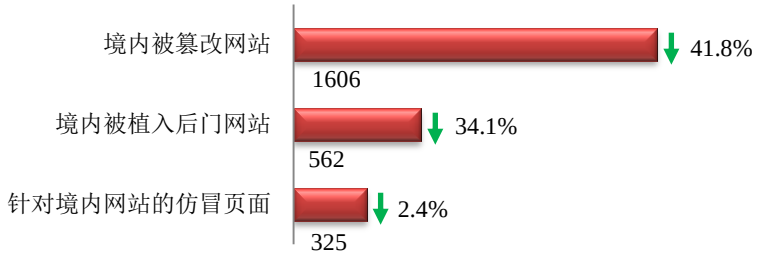
ANVA恶意地址黑名单发布地址

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。

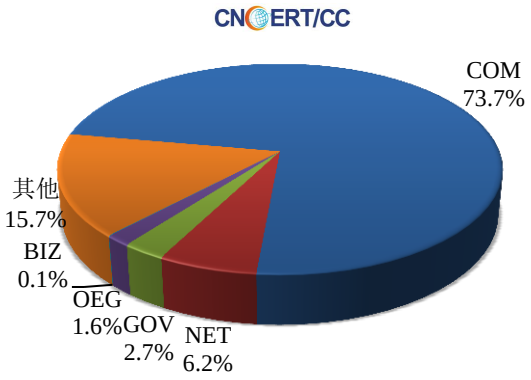
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1606 个；境内被植入后门的网站数量为 562 个；针对境内网站的仿冒页面数量为 325。

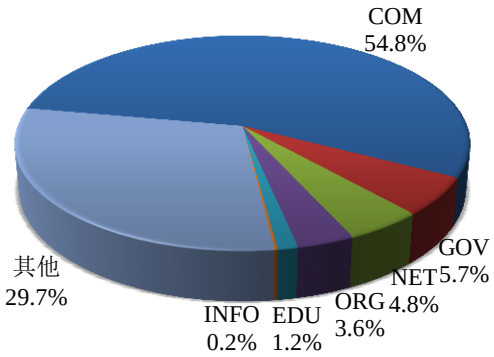


本周境内被篡改政府网站（GOV 类）数量为 44 个（约占境内 2.7%），较上周环比下降了 31.3%；境内被植入后门的政府网站（GOV 类）数量为 32 个（约占境内 5.7%），较上周环比下降了 23.8%；针对境内网站的仿冒页面涉及域名 275 个，IP 地址 197 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(10/16-10/22)

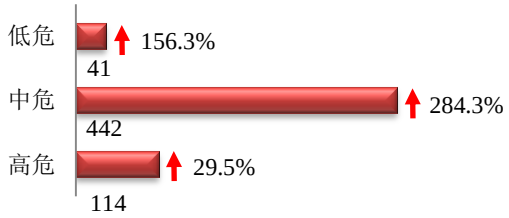


本周我国境内被植入后门网站按类型分布
(10/16-10/22)

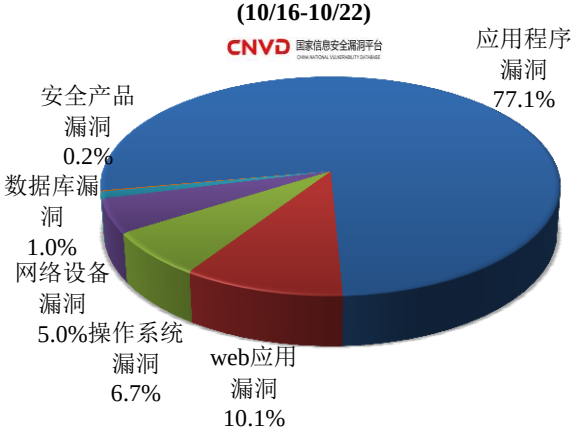


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 597 个，信息安全漏洞威胁整体评价级别为高。



本周CNVD收录漏洞按影响对象类型分布
(10/16-10/22)



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 应用漏洞和操作系统漏洞。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

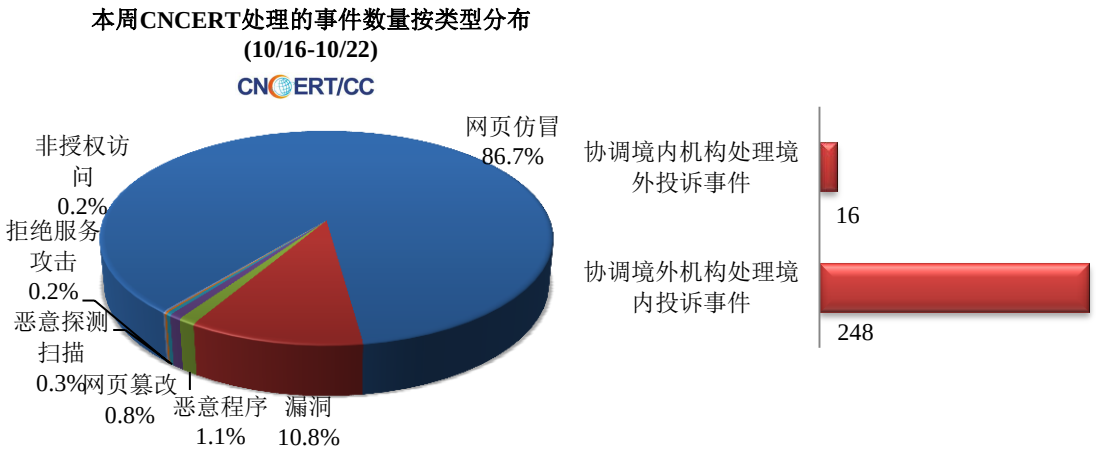
CNVD漏洞周报发布地址

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。

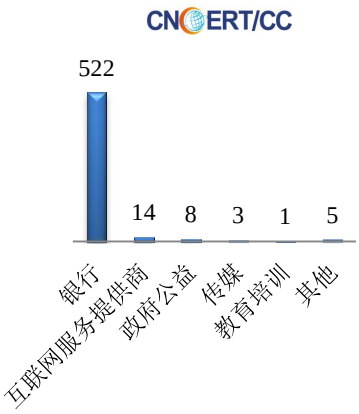
本周事件处理情况

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 638 起，其中跨境网络安全事件 264 起。

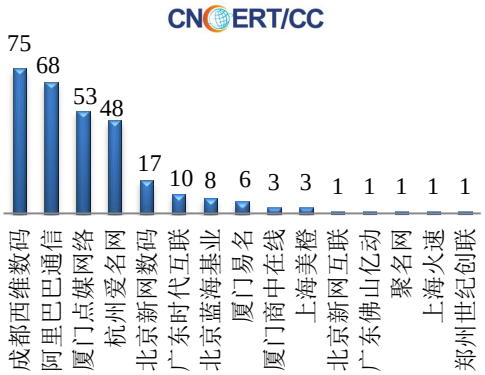


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 553 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 522 起和互联网服务提供商仿冒事件 14 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(10/16-10/22)

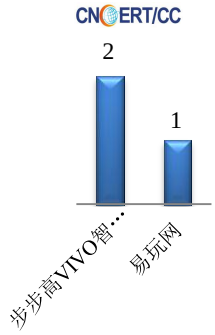


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (10/16-10/22)



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 3 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 (10/16-10/22)



业界新闻速递

1、第二届内地-香港网络安全论坛成功举办

中国网 10 月 18 日消息 2017 年 10 月 15 日，第二届内地-香港网络安全论坛在厦门市成功举办，中央网信办网络安全协调局局长赵泽良、香港特区政府资讯科技总监杨德斌出席，来自两地政府、高校和产业界的约 150 名专家代表参加了论坛。论坛邀请了北京大学、四川大学、中国电子技术标准化研究院，以及香港个人资料私隐专员公署、智能城市联盟数据产业委员会的专家，围绕两地数据安全保护政策法律、个人信息保护标准与实践、网络安全人才培养等共同关心的话题，同两地代表进行了交流讨论，分享了经验做法。

2、美国联邦能源监管机构（FERC）将采取行动改善电网安全

HackerNews.cc10 月 21 日消息 随着国家对网络攻击的日益关注，其关键基础设施越来越需要保护。美国能源部曾于 2017 年 1 月发布的《Quadrennial Energy Review》中写道：“黑客对电力系统的威胁日益复杂，其规

模和频率都在不断增加。目前，电力系统的可靠性几乎支撑了现代美国经济的每一个领域。为应对此类攻击，美国联邦能源管理委员会（FERC）近期提出新网络安全管理控制措施，以增强国家电力系统的可靠性与弹性。目前，FERC 提议批准关键基础设施保护（CIP）的可靠性指标 CIP-003-7（网络安全-安全管理控制），旨在降低可能影响电力系统运行的网络安全风险。据悉，新指标将特别改进现有的访问控制标准：阐明适用于低影响网络系统的电子访问控制义务，对临时电子设备（如 thumb 驱动器和笔记本电脑）采取强制性安全控制，制定实体宣传和回应 CIP 与低影响网络系统有关的特殊政策。

3、美国土安全局要求所有联邦机构在其电邮系统中部署 DMARC

cnBeta.COM10 月 17 日消息 据外媒报道，当地时间周一，美国国土安全局（DHS）宣布了一项针对冒名顶替的政府电子邮件的举措。在未来的 90 天内，所有联邦机构都将要在其系统内部署 DMARC 邮件安全功能。DMARC 全称 Domain-based Message Authentication, Reporting and Conformance，即基于域名的消息认证、报告以及一致性。大多数消费类电子邮件系统都采用了这项功能。今年 7 月，俄勒冈州民主党参议员 Ron Wyden 就曾写信给 DHS 网络安全与通信办公室的 Jeanett Manfra 要求在联邦机构中部署 DMARC。今年 5 月，一起假装五角大楼的欺诈邮件网络攻击发生。而在 2015 年至 2016 年之间，国税局遭到的冒名网络攻击事件数量增加了 4 倍。Manfra 指出，DMARC 将能阻止这种冒名邮件的网络攻击。另外，DHS 还要求所有联邦机构的网站都用上 HTTPS。获悉，仍有近 1/4 的联邦政府网站还没有开始使用 HTTPS。

4、俄罗斯将开始对虚拟货币挖矿行为展开监管

cnBeta.COM10 月 18 日消息 据外媒报道，在决定推出自己的虚拟货币 CryptoRuble 之后，现在，俄罗斯联邦政府又作出了禁止虚拟货币挖矿行为的决定。俄通信部长 Nikolay Nikiforov 指出，虚拟货币必须不能作为私人货币存在，它将由国家发行、控制，与此同时它能够在数字经济中提供数字货币流通。目前还不清楚这一决定将对比特币等虚拟货币的影响。不过由于俄罗斯方面并没有以禁止其他虚拟货币的使用，所以它带来的影响范围可能不会太大。据了解，实体卢比和虚拟货币 CryptoRuble 将能相互兑换，但如果兑换者无法解释来源的话政府将需要对其征收 13%的税收。此外，如果两者之间出现价格差，那么政府将通过征税的形式弥补这一差价，进而使这两者保持在同一水平。

5、南非史上最大数据泄露事件：3000 万公民信息暴露于互联网上

E 安全 20 月 20 日消息 据外媒 10 月 18 日报道，网络安全专家近期发现一份逾 27G 转储文件，其包含 3000 万南非公民的身份号码、个人收入、年龄、就业历史、公司董事身份、种族群体、婚姻状况、职业、雇主和家庭地址等敏感信息。知名媒体 iafrikan 透露，该批数据来源于 Dracore Data Sciences 企业的 GoVault 平台，其公司客户包括南非最大的金融信贷机构——TransUnion。随后，安全研究人员经调查后发现该公司将用户数据发布到一台完全未经保护的 Web 服务器上，其允许任意用户进行访问。研究人员表示，这可能是南非最大的一次数据泄露事件。虽然尚未发现数据已被黑客利用，但这可能只是时间上的问题。

6、WiFi 漏洞几乎影响所有无线设备

新浪网 10 月 17 日消息 北京时间 10 月 17 日早间消息，有计算机安全专家发现了 WiFi 设备的安全协议存

在漏洞。这个漏洞影响许多设备，比如计算机、手机、路由器，几乎每一款无线设备都有可能被攻击。漏洞名叫“KRACK”，也就是“Key Reinstallation Attack”（密钥重安装攻击）的缩写，它曝露了 WPA2 的一个基本漏洞，WPA2 是一个通用协议，大多现代无线网络都用到了该协议。计算机安全学者马蒂 •凡赫尔夫（Mathy Vanhoef）发现了漏洞，他说漏洞存在于四路握手（four-way handshake）机制中，四路握手允许拥有预共享密码的新设备加入网络。在最糟糕的情况下，攻击者可以利用漏洞从 WPA2 设备破译网络流量、劫持链接、将内容注入流量中。换言之，攻击者通过漏洞可以获得一个万能密钥，不需要密码就可以访问任何 WAP2 网络。一旦拿到密钥，他们就可以窃听你的网络信息。漏洞的存在意味着 WAP2 协议完全崩溃，影响个人设备和企业设备，几乎每一台设备都受到威胁。

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：周昊

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158