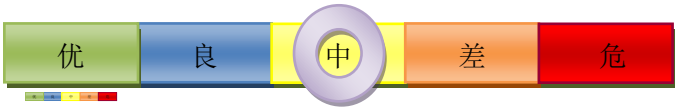
CNCERT互联网安全威胁报告

2019 年 9 月　　总第 105 期



摘要：

本报告以 CNCERT 监测数据和通报成员单位报送数据作为主要依据，对我国互联网面临的各类安全威胁进行总体态势分析，并对重要预警信息和典型安全事件进行探讨。

2019 年 9 月，互联网网络安全状况整体评价为中。主要数据如下：

- 境内感染网络病毒的终端数为近175万余个；
- 境内被篡改网站数量为52,521个，其中被篡改政府网站数量为43个；境内被植入后门的网站数量为12,788个，其中政府网站有106个；针对境内网站的仿冒页面数量为190个；
- 国家信息安全漏洞共享平台（CNVD）收集整理信息系统安全漏洞2,003个。其中，高危漏洞546个，可被利用来实施远程攻击的漏洞有1,765个。

热线电话：+8610 82990999（中文），82991000（英文） 传真：+8610 82990399

电子邮件：cncert@cert.org.cn

PGP Key：http://www.cert.org.cn/cncert.asc

网址：http://www.cert.org.cn/

关于国家计算机网络应急技术处理协调中心（CNCERT）

1、CNCERT 简介

工作职责

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称 CNCERT 或 CNCERT/CC），成立于 2001 年 8 月，为非政府非盈利的网络安全技术中心，是中国计算机网络应急处理体系中的牵头单位。作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护公共互联网安全，保障关键信息基础设施的安全运行。

应急体系

CNCERT 在中国大陆 31 个省、自治区、直辖市设有分支机构。目前，CNCERT 作为中国计算机网络应急处理体系中的牵头单位，通过组织网络安全企业、学校、社会组织和研究机构，协调骨干网络运营单位、域名服务机构和其他应急组织等，构建中国互联网安全应急体系，共同处理各类互联网重大网络安全事件。

行业合作

CNCERT 积极发挥行业联动合力，发起成立了国家信息安全漏洞共享平台（CNVD）、中国反网络病毒联盟（ANVA）和中国互联网网络安全威胁治理联盟（CCTGA），与国内的基础电信企业、增值电信企业、域名注册服务机构、网络安全服务厂商等建立漏洞信息共享、网络病毒防范、威胁治理和情报共享等工作机制，加强网络安全信息共享和技术合作。CNCERT 还通过公开选拔方式，选择部分在中国境内从事公共互联网网络安全服务的机构作为“CNCERT 网络安全应急服务支撑单位”。在 CNCERT 的统一协调与指导下，各支撑单位共同参与中国互联网安全事件的应急处理工作，维护公共互联网网络安全。

国际合作

CNCERT 积极开展网络安全国际合作，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，是国际著名网络安全合作组织 FIRST 的正式成员，以及亚太应急组织 APCERT 的发起者之一。CNCERT 持续实施“CNCERT 国际合作伙伴计划”，已与百余个组织建立了联系机制。CNCERT 还积极参加亚太经合组织、国际电联、上合组织、东盟、金砖等政府层面国际和区域组织的网络安全相关工作。

2、业务范围

事件发现：CNCERT 依托公共互联网网络安全监测平台开展对基础信息网络、金融证券等重要信息系统、移动互联网服务提供商、增值电信企业等安全事件的自主监测。同时还通过与国内外合作伙伴进行数据和信息共享，以及通过热线电话、传真、电子邮件、网站等接收国内外用户的网络安全事件报告等多种渠道发现网络攻击威胁和网络安全事件。

预警通报：CNCERT 依托对丰富数据资源的综合分析和多渠道的信息获取实现网络安全威胁的分析预警、网络安全事件的情况通报、宏观网络安全状况的态势分析等，为用户单位提供互联网网络安全态势信息通报、网络安全技术和资源信息共享等服务。

应急处置：对于自主发现和接收到的危害较大的事件报告，CNCERT 及时响应并积极协调处置，重点处置的事件包括：影响互联网运行安全的事件、波及较大范围互联网用户的事件、涉及重要政府部门和重要信息系统的事件、用户投诉造成较大影响的事件，以及境外国家级应急组织投诉的各类网络安全事件等。

测试评估：作为网络安全检测、评估的专业机构，按照“支撑监管，服务社会”的原则，以科学的方法、规范的程序、公正的态度、独立的判断，按照相关标准为政府部门、企事业单位提供安全评测服务。CNCERT 还组织通信网络安全相关标准制定，参与电信网和互联网安全防护系列标准的编制等。

版权及免责声明

编者按：

感谢您阅读《CNCERT 互联网安全威胁报告》，如果您发现本报告存在任何问题，请您及时与我们联系，来信地址为：cncert@cert.org.cn。

本月网络安全基本态势分析

2019 年 9 月，互联网网络安全状况整体评价为中。我国基础网络运行总体平稳，互联网骨干网各项监测指标正常，未发生较大以上网络安全事件。在我国互联网网络安全环境方面，境内感染木马或僵尸程序的 IP 地址数目、境内被植入后门的网站数量和漏洞报告数量较上月有所增长，其他各类网络安全事件数量均有不同程度的下降。总体上，9 月公共互联网网络安全态势较上月有所好转。

◆ 基础网络安全

2019 年 9 月，我国基础网络运行总体平稳，互联网骨干网各项监测指标正常，未出现省级行政区域以上的造成较大影响的基础网络运行故障，未发生较大以上网络安全事件。

◆ 关键信息基础设施安全

本月，监测发现境内政府网站被篡改的数量为 43 个，与上月的 113 个相比下降 61.9%，占境内被篡改网站的比例与上月持平；境内政府网站被植入后门的数量为 106 个，与上月的 90 个相比增长 17.8%，占境内被植入后门网站的比例与上月持平。国家信息安全漏洞共享平台（CNVD）共协调处置了 1909 起涉及我国政府部门以及银行、民航等重要信息系统部门以及电信、传媒、公共卫生、教育等相关行业的漏洞事件。

◆ 公共网络环境安全

2019 年 9 月，根据 CNCERT 的监测数据，我国互联网网络安全环境主要指标情况如下：网络病毒[1]活动情况方面，境内感染网络病毒

注1：一般情况下，恶意代码是指在未经授权的情况下，在信息系统中安装、执行以达到不正当目的的程序。其中，网络病毒是特指有网络通信行为的恶意代码。9 月，CNCERT 在对恶意代码进行抽样监测时，对 551 种木马家族和 83 种僵尸程序家族进行了抽样监测。

的终端数为 175 万余个，较上月增长 35.2%。网站安全方面，境内被篡改网站数量为 52,521，较上月下降 47.1%；境内被植入后门的网站数量为 12,788 个，较上月增长 9.7%。针对境内网站的仿冒页面数量为 196 个，较上月下降 86.4%。安全漏洞方面，本月 CNVD 共收集整理信息系统安全漏洞 2,003 个，较上月增长 10.0%。其中高危漏洞 546 个，较上月增长 22.7%；可被利用来实施远程攻击的漏洞有 1,765 个，较上月增长 13.7%。事件受理方面，CNCERT 接收到网络安全事件报告 9,334 件，较上月下降 0.8%，数量最多的分别是漏洞类事件 3,581 件、恶意程序类事件 2,297 件。事件处理方面，CNCERT 处理了网络安全事件 9,294 件，数量最多的分别是漏洞类事件 3,536 件、恶意程序类事件 2,298 件。

本月网络安全主要数据

◆ 网络病毒监测数据分析

2019 年 9 月，境内感染网络病毒的终端数为 175 万余个。其中，境内近 150 万个 IP 地址对应的主机被木马或僵尸程序控制，与上月的近 103 万个相比增长 45.7%。

➢ *木马僵尸网络监测数据分析*

2019 年 9 月，境内近 150 万个 IP 地址对应的主机被木马或僵尸程序控制，按地区分布感染数量排名前三位的分别是江苏省、浙江省、广东省。

木马或僵尸网络控制服务器 IP 总数为 7,382 个。其中，境内木马或僵尸程序控制服务器 IP 有 2,221 个，按地区分布数量排名前三位的分别为广东省、北京市、江苏省。境外木马或僵尸程序控制服务器 IP 有 5, 161 个，主要分布于美国、中国香港和荷兰。其中，位于美国的控制服务器控制了境内 1,068,846 个主机 IP，控制境内主机 IP 数量居首位，其次是位于荷兰和法国的 IP 地址，分别控制了境内 710,532 个和 327,042 个主机 IP。

➢ *移动互联网恶意程序监测数据分析*

2019 年 9 月，CNCERT 重点针对目前流行的信息窃取类、恶意扣费类和敲诈勒索类典型移动恶意程序进行分析，发现敲诈勒索类恶意程序样本 150 个，恶意扣费类恶意程序样本 405 个，信息窃取类恶意程序样本 506 个。

2019 年 9 月，CNCERT 向应用商店、个人网站、广告平台、云平台等传播渠道通报下架移动互联网恶意程序 202 个。这些移动互联网恶意程序按行为属性统计，流氓行为类的资费消耗数量居首位(占

25.2%)，恶意扣费类（占 24.8%）、流氓行为类（占 24.8%）分列第二、三位。

➢ 网络病毒捕获和传播情况

网络病毒主要针对一些防护比较薄弱，特别是访问量较大的网站通过网页挂马的方式进行传播。当存在安全漏洞的用户主机访问了这些被黑客挂马的网站后，会经过多级跳转暗中连接黑客最终“放马”的站点下载网络病毒。

网络病毒在传播过程中，往往需要利用黑客注册的大量域名。2019 年 9 月，CNCERT 监测发现的放马站点中，通过域名访问的共涉及有 5,921 个域名，通过 IP 直接访问的共涉及有 14,188 个 IP。在 5,921 个放马站点域名中，于境内注册的域名数为 1,820 个（约占 30.7%），于境外注册的域名数为 792 个（约占 13.4%）。放马站点域名所属顶级域名排名前 5 位的具体情况如表所示。

表 2019 年 9 月活跃恶意域名所属顶级域名

排序	顶级域名（TLD）	类别	恶意域名数量
1	.COM	通用顶级域名（gTLD）	1981
2	.CN	国家顶级域名（ccTLD）	894
3	.IO	通用顶级域名（gTLD）	190
4	.NET	通用顶级域名（gTLD）	189
5	.ORG	通用顶级域名（gTLD）	67

◆ 网站安全数据分析

➢ 境内网站被篡改情况

2019 年 9 月，境内被篡改网站的数量为 52,521 个，境内被篡改网站数量按地区分布排名前三位的分别是北京市、山东省和广东省。按网站类型统计，被篡改数量最多的是.COM 域名类网站，其多为商业类网站；被篡改的.GOV 域名类网站有 43 个，占境内被篡改网站的比例为 0.1%。

➢ 境内网站被植入后门情况

2019 年 9 月，境内被植入后门的网站数量为 12,788 个，境内被植入后门的网站数量按地区分布排名前三位的分别是北京市、广东省、河南省。按网站类型统计，被植入后门数量最多的是.COM 域名类网站；被植入后门的.GOV 域名类网站有 106 个，占境内被植入后门网站的比例为 0.8%。

2019 年 9 月，境外 8,114 个 IP 地址通过植入后门对境内 12,370 个网站实施远程控制。其中，境外 IP 地址主要位于美国、新加坡和中国香港等国家或地区。从境外 IP 地址通过植入后门控制境内网站数量来看，来自菲律宾的 IP 地址共向境内 3,586 个网站植入了后门程序，入侵网站数量居首位；其次是来自美国和中国香港的 IP 地址，分别向境内 3,103 个和 2,923 个网站植入了后门程序。

➢ 境内网站被仿冒情况

2019 年 9 月，CNCERT 共监测到针对境内网站的仿冒页面有 190 个，涉及域名 114 个，IP 地址 94 个，在这 94 个 IP 中，100%位于境外，主要位于中国香港和美国。

◆ 漏洞数据分析

2019 年 9 月，CNVD 收集整理信息系统安全漏洞 2,003 个。其中，高危漏洞 546 个，可被利用来实施远程攻击的漏洞 1,765 个。受影响的软硬件系统厂商包括 Adobe、Cisco、Google、IBM、Microsoft、Moxa、Mozilla、Oracle 等。

根据漏洞影响对象的类型，漏洞可分为应用程序、WEB 应用、操作系统、网络设备（交换机、路由器等网络端设备）、安全产品（如防火墙、入侵检测系统等）、数据库和智能设备（物联网终端设备）漏洞。本月 CNVD 收集整理的漏洞中，按漏洞类型分布排名前三位的分别是应用程序漏洞、WEB 应用漏洞、操作系统漏洞。

◆ 网络安全事件接收与处理情况

➢ *事件接收情况*

2019 年 9 月，CNCERT 收到国内外通过电子邮件、热线电话、网站提交、传真等方式报告的网络安全事件 9,334 件（合并了通过不同方式报告的同一网络安全事件，且不包括扫描和垃圾邮件类事件），其中来自国外的事件报告有 23 件。

在 9,334 件事件报告中，排名前三位的安全事件分别是漏洞、恶意程序、网页篡改类事件。

➢ *事件处理情况*

对国内外通过电子邮件、热线电话、传真等方式报告的网络安全事件，以及自主监测发现的网络安全事件，CNCERT 每日根据事件的影响范围和存活性、涉及用户的性质等因素，筛选重要事件进行协调处理。

2019 年 9 月，CNCERT 以及各省分中心共同协调处理了 9,294 起安全事件。其中漏洞类、恶意程序类事件处理数量较多。

附：术语解释

- 信息系统

信息系统是指由计算机硬件、软件、网络和通信设备等组成的以处理信息和数据为目的的系统。

- 漏洞

漏洞是指信息系统中的软件、硬件或通信协议中存在缺陷或不适当的配置，从而可使攻击者在未授权的情况下访问或破坏系统，导致信息系统面临安全风险。

- 恶意程序

恶意程序是指在未经授权的情况下，在信息系统中安装、执行以达到不正当目的的程序。恶意程序分类说明如下：

1. 特洛伊木马（Trojan Horse）

   特洛伊木马（简称木马）是以盗取用户个人信息，甚至是远程控制用户计算机为主要目的的恶意代码。由于它像间谍一样潜入用户的电脑，与战争中的“木马”战术十分相似，因而得名木马。按照功能，木马程序可进一步分为：盗号木马[2]、网银木马[3]、窃密木马[4]、远程控制木马[5]、流量劫持木马[6]、下载者木马[7]和其它木马七类。

2. 僵尸程序（Bot）

   僵尸程序是用于构建大规模攻击平台的恶意代码。按照使用的通信协议，僵尸程序可进一步分为：IRC 僵尸程序、Http 僵尸程序、P2P 僵尸程序和其它僵尸程序四类。

3. 蠕虫（Worm）

   蠕虫是指能自我复制和广泛传播，以占用系统和网络资源为主要目的的恶意代码。按照传播途径，蠕虫可进一步分为：邮件蠕虫、即时消息蠕

注2：盗号木马是用于窃取用户电子邮箱、网络游戏等账号的木马。

注3：网银木马是用于窃取用户网银、证券等账号的木马。

注4：窃密木马是用于窃取用户主机中敏感文件或数据的木马。

注5：远程控制木马是以不正当手段获得主机管理员权限，并能够通过网络操控用户主机的木马。

注6：流量劫持木马是用于劫持用户网络浏览的流量到攻击者指定站点的木马。

注7：下载者木马是用于下载更多恶意代码到用户主机并运行，以进一步操控用户主机的木马。

虫、U 盘蠕虫、漏洞利用蠕虫和其它蠕虫五类。

4. 病毒（Virus）

病毒是通过感染计算机文件进行传播，以破坏或篡改用户数据，影响信息系统正常运行为主要目的恶意代码。

5. 其它

上述分类未包含的其它恶意代码。

随着黑客地下产业链的发展，互联网上出现的一些恶意代码还具有上述分类中的多重功能属性和技术特点，并不断发展。对此，我们将按照恶意代码的主要用途参照上述定义进行归类。

- 僵尸网络

僵尸网络是被黑客集中控制的计算机群，其核心特点是黑客能够通过一对多的命令与控制信道操纵感染木马或僵尸程序的主机执行相同的恶意行为，如可同时对某目标网站进行分布式拒绝服务攻击，或发送大量的垃圾邮件，或进行“挖矿”等。

- 拒绝服务攻击

拒绝服务攻击是向某一目标信息系统发送密集的攻击包，或执行特定攻击操作，以期致使目标系统停止提供服务。

- 网页篡改

网页篡改是恶意破坏或更改网页内容，使网站无法正常工作或出现黑客插入的非正常网页内容。

- 网页仿冒

网页仿冒是通过构造与某一目标网站高度相似的页面（俗称钓鱼网站），并通常以垃圾邮件、即时聊天、手机短信或网页虚假广告等方式发送声称来自于被仿冒机构的欺骗性消息，诱骗用户访问钓鱼网站，以获取用户个人秘密信息（如银行帐号和帐户密码）。

- 网页挂马

网页挂马是通过在网页中嵌入恶意代码或链接，致使用户计算机在访问该页面时被植入恶意代码。

- 网站后门

网站后门事件是指黑客在网站的特定目录中上传远程控制页面从而能够通

过该页面秘密远程控制网站服务器的攻击事件。

- 垃圾邮件

垃圾邮件是将不需要的消息（通常是未经请求的广告）发送给众多收件人。包括：（一）收件人事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等宣传性的电子邮件；（二）收件人无法拒收的电子邮件；（三）隐藏发件人身份、地址、标题等信息的电子邮件；（四）含有虚假的信息源、发件人、路由等信息的电子邮件。

- 域名劫持

域名劫持是通过拦截域名解析请求或篡改域名服务器上的数据，使得用户在访问相关域名时返回虚假 IP 地址或使用户的请求失败。

- 非授权访问

非授权访问是没有访问权限的用户以非正当的手段访问数据信息。非授权访问事件一般发生在存在漏洞的信息系统中，黑客利用专门的漏洞利用程序（Exploit）来获取信息系统访问权限。

- 移动互联网恶意程序

在用户不知情或未授权的情况下，在移动终端系统中安装、运行以达到不正当目的，或具有违反国家相关法律法规行为的可执行文件、程序模块或程序片段。