



CNCERT互联网安全威胁报告

2018年3月 总第87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。

2018年3月，互联网网络安全状况整体评价为良。主要数据如下：

- 境内感染网络病毒的终端数为75万余个；
- 境内被篡改网站数量为2,559个，其中被篡改政府网站数量为57个；境内被植入后门的网站数量为2,858个，其中政府网站有73个；针对境内网站的仿冒页面数量为3,791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洞1,902个，其中，高危漏洞598个，可被用来实施远程攻击的漏洞有1,631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，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

2003年，CNCERT在全国31个省（直辖市、自治区）成立分中心。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，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

CNCERT的业务能力如下：

事件发现——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——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。

同时，作为中国非政府层面开展网络安全事件跨境处置协助的重要窗口，CNCERT积极开展国际合作，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。CNCERT为国际著名网络安全合作组织FIRST正式成员以及亚太应急组织APCERT的发起人之一。截止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。

版权及免责声明

《CNCERT 互联网安全威胁报告》(以下简称“报告”)为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, CNCERT 或 CNCERT/CC)的电子刊物,由 CNCERT 编制并拥有版权。报告中凡摘录或引用内容均已指明出处,其版权归相应单位所有。本报告所有权利及许可由 CNCERT 进行管理,未经 CNCERT 同意,任何单位或个人不得将本报告以及其中内容转发或用于其他用途。

CNCERT 力争保证本报告的准确性和可靠性,其中的信息、数据、图片等仅供参考,不作为您个人或您企业实施安全决策的依据, CNCERT 不承担与此相关的一切法律责任。

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

2018年3月，互联网网络安全状况整体评价为良。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，除境内被篡改网站的总数和自主监测发现的我国大陆被篡改网站的数量较上月有所下降，其他各类网络安全事件数量均有不同程度的增长。总体上，3月公共互联网网络安全态势较上月有所恶化，但评价指数在良的区间。

◆ 基础网络安全

2018年3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。

◆ 重要联网信息系统安全

本月，监测发现境内政府网站被篡改的数量为57个，与上月的53个相比增长7.5%，占境内被篡改网站的比例由1.4%上升到2.2%；境内政府网站被植入后门的数量为73个，与上月的28个相比增长160.7%，占境内被植入后门网站的比例由1.6%上升到2.6%；针对境内网站的仿冒页面数量为3,791个，较上月的583个增长550.3%。国家信息安全漏洞共享平台（CNVD¹）共协调处置了1,868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

2018年3月，根据CNCERT的监测数据和通信行业报送数据，

注1：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，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

我国互联网网络安全环境主要指标情况如下：网络病毒²活动情况方面，境内感染网络病毒的终端数为 75 万余个，较上月增长 45.6%；各安全企业报送的恶意代码捕获数量中，瑞星公司截获的病毒数量较上月增长 27.8%，新增病毒数量较上月增长 2.6%；安天公司捕获的样本总数较上月增长 11.3%，新增病毒种类较上月增长 68.8%；猎豹移动报送的计算机病毒事件数量较上月增长 9.8%。网站安全方面，境内被篡改网站数量为 2,559 个，较上月下降 30.4%；境内被植入后门的网站数量为 2,858 个，较上月增长 66.4%；针对境内网站的仿冒页面有 3,791 个，较上月增长 550.3%；各安全企业报送的网页挂马情况中，奇虎 360 公司报送的网页挂马事件数量较上月下降 33.3%。安全漏洞方面，本月 CNVD 共收集整理信息系统安全漏洞 1,902 个，较上月增长 130.8%。其中高危漏洞 598 个，较上月增长 114.3%；可被利用来实施远程攻击的漏洞有 1,631 个，较上月增长 146.0%。事件受理方面，CNCERT 接收到网络安全事件报告 9,650 件，较上月增长了 39.6%。数量最多的分别是漏洞类事件 3,283 件、网页仿冒类事件 3,075 件。事件处理方面，CNCERT 处理了网络安全事件 9,751 件，数量最多的分别是漏洞类事件 3,297 件、网页仿冒类事件 3,134 件。

注2：一般情况下，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。1 月，CNCERT 在对恶意代码进行抽样监测时，对 545 种木马家族和 80 种僵尸程序家族进行了抽样监测。

本月重点网络安全信息

◆ 通报 Memcached 服务器反射攻击情况

针对近期呈大幅上升趋势的 Memcached 服务器反射攻击事件，CNCERT 有序开展应急响应工作，并于 3 月 3 日、3 月 9 日持续向公众进行预警通报。截止 3 月 9 日，CNCERT 通报处置了 13981 个已被利用发起攻击或探测扫描的 Memcached 服务器。在 Memcached 服务器反射流量分析方面，CNCERT 抽样监测发现，3 月 1 日全网 Memcached 服务器反射攻击流量达到高峰后，3 月 2 日至 4 日有所回落，但 3 月 5 至 7 日反射攻击峰值流量又上升接近 500GB。CNCERT 将密切关注 Memcached 服务器反射攻击的演变情况，并进行持续通报。

◆ CNCERT 圆满完成 2018 年 APCERT 应急演练

2018 年 3 月 7 日，CNCERT/CC 参加了亚太地区计算机应急响应组织（APCERT）发起举办的 2018 年亚太地区网络安全应急演练，圆满完成了各项演练任务。本次演练主题是“物联网上恶意软件导致的数据泄露”，是基于互联网上真实存在的事件与情况，模拟医疗机构受网络攻击的场景，分析并协调处置由恶意软件引发的医疗机构的数据渗透和物联网设备感染事件。来自 20 个经济体（澳大利亚、孟加拉国、文莱、中国、中国台北、中国香港、印度、印尼、日本、韩国、老挝、中国澳门、马来西亚、蒙古、缅甸、新西兰、新加坡、斯里兰卡、泰国和越南）的 27 个 CSIRT 成员参加了此次演练。此外，本次演练第五次邀请了伊斯兰计算机应急响应合作组织（OIC-CERT）的成员参加，来自 5 个经济体（埃及、摩洛哥、尼日利亚、阿曼、巴基斯坦）的 OIC-CERT 成员参加了演练。

◆ 通报 Exim SMTP Mail Server 存在缓冲区溢出漏洞

3月，CNVD收录了 Exim SMTP Mail Server 缓冲区溢出漏洞³。攻击者可利用该漏洞在受影响的应用程序上下文中，通过堆溢出实现代码的执行，若攻击尝试失败仍可导致拒绝服务条件。该漏洞是源于 Exim 4.90.1 之前版本中 SMTP 侦听器'base64d()'解码函数在发送 handcrafted 消息时存在缓冲区溢出漏洞，由于 Exim 未能充分检查用户提供的数据，受影响也是 Exim 4.90.1 之前的版本。厂商已发布漏洞修复版本，下载地址：https://www.exim.org/mirmon/ftp_mirrors.html。目前，漏洞利用代码已公开，建议及时更新到漏洞修复后版本。

◆ 通报 Drupal core 远程代码执行漏洞

3月，CNVD收录了 Drupal core 远程代码执行漏洞⁴。综合利用该漏洞，攻击者可实现远程代码执行攻击。Drupal 是一个由 Dries Buytaert 创立的自由开源的内容管理系统，用 PHP 语言写成。在业界 Drupal 常被视为内容管理框架，而非一般意义上的内容管理系统，此次曝出的漏洞将影响到 Drupal 的 6.x，7.x 和 8.x 版本。根据 CNVD 统计情况，全球系统规模约为 30.9 万，用户量排名前五的分别是美国(48.5%)、德国(8.1%)、法国(4%)、英国(3.8%)和俄罗斯(3.7%)，而在我国境内的分布较少(0.88%)。目前，漏洞细节尚未公开，CNVD 提出了详细修复建议，具体可参考 CNVD 发布的安全公告 http://www.cert.org.cn/publish/main/9/2018/20180330135822851987471/20180330135822851987471_.html。

注 3：CNVD-2018-04619，对应 CVE-2018-6789。

注 4：CNVD-2018-06660，对应 CVE-2018-7600。

本月网络安全主要数据

◆ 网络病毒监测数据分析

2018年3月，境内感染网络病毒的终端数为75万余个。其中，境内42万余个IP地址对应的主机被木马或僵尸程序控制，与上月的近29万个相比增长47.5%。

➤ 木马僵尸网络监测数据分析

2018年3月，境内42万余个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浙江省、河南省、广东省。

木马或僵尸网络控制服务器IP总数为17,563个。其中，境内木马或僵尸程序控制服务器IP有2,259个，按地区分布数量排名前三位的分别为广东省、北京市、浙江省。境外木马或僵尸程序控制服务器IP有15,304个，主要分布于美国、越南、日本。其中，位于美国的控制服务器控制了境内224,952个主机IP，控制境内主机IP数量居首位，其次是位于中国香港和加拿大的IP地址，分别控制了境内50,741个和14,351个主机IP。

➤ 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。2018年3月，CNCERT监测发现排名前十的活跃放马站点域名和活跃放马站点IP如表1所示。

表1：2018年3月活跃放马站点域名和IP

排序	活跃放马站点域名	排序	活跃放马站点IP
1	www.go890.com	1	117.23.6.63
2	cl.urndf.com	2	120.26.127.170

3	dl.urndf.com	3	220.181.105.173
4	down.nxwb.net	4	122.72.35.190
5	dxdown.nonglirili.net	5	61.133.194.190
6	cl.qpzqxz.com	6	117.23.6.64
7	url.222bz.com	7	117.23.6.65
8	rkverify.securestudies.com	8	111.161.3.176
9	dl.aplx.com	9	171.111.154.225
10	cl.aplx.com	10	117.131.204.56

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。2018年3月，CNCERT监测发现的放马站点中，通过域名访问的共涉及有39个域名，通过IP直接访问的共涉及有45个IP。在39个放马站点域名中，于境内注册的域名数为27个（约占69.2%），于境外注册的域名数为12个（约占30.8%）。放马站点域名所属顶级域名排名前5位的具体情况如表2所示。

表2：2018年3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)	27
2	.NET	通用顶级域名(gTLD)	7
3	.CN	国家顶级域名(ccTLD)	3
4	.INFO	通用顶级域名(gTLD)	1
5	.CC	通用顶级域名(gTLD)	1

◆ 网站安全数据分析

➤ 境内网站被篡改情况

2018年3月，境内被篡改网站的数量为2,559个，境内被篡改网站数量按地区分布排名前三位的分别是广东省、北京市、浙江省。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；值得注意的是，被篡改的.GOV域名类网站有57个，占境内被篡改网站的比例为2.2%。

➤ 境内网站被植入后门情况

2018年3月,境内被植入后门的网站数量为2,858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广东省、北京市、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,其多为商业类网站;值得注意的是,被植入后门的.GOV域名类网站有73个,占境内被植入后门网站的比例为2.6%。

2018年3月,境外2,597个IP地址通过植入后门对境内2,858个网站实施远程控制。其中,境外IP地址主要位于美国、中国香港和俄罗斯等国家或地区。从境外IP地址通过植入后门控制境内网站数量来看,来自乌克兰的IP地址共向境内526个网站植入了后门程序,入侵网站数量居首位;其次是来自中国香港和俄罗斯的IP地址,分别向境内487个和383个网站植入了后门程序。

➤ 境内网站被仿冒情况

2018年3月,CNCERT共监测到针对境内网站的仿冒页面有3,791个,涉及域名2,046个,IP地址428个,平均每个IP地址承载近9个仿冒页面。在这428个IP中,98.1%位于境外,主要位于中国香港和美国。

◆ 漏洞数据分析

2018年3月,CNVD收集整理信息系统安全漏洞1,902个。其中,高危漏洞598个,可被利用来实施远程攻击的漏洞有1,631个。受影响的软硬件系统厂商包括Adobe、Cisco、Drupal、Google、IBM、Linux、Microsoft、Mozilla、WordPress等。

根据漏洞影响对象的类型,漏洞可分为操作系统漏洞、应用程序漏洞、WEB应用漏洞、数据库漏洞、网络设备漏洞(如路由器、交换机等)和安全产品漏洞(如防火墙、入侵检测系统等)。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

2018年3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9,650件（合并了通过不同方式报告的同—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25件。

在9,650件事件报告中，排名前三位的安全事件分别是漏洞、网页仿冒、恶意程序。

➤ 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。

2018年3月，CNCERT以及各省分中心共同协调处理了9,751件网络安全事件。各类事件处理数量中漏洞、网页仿冒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⁵、网银木马⁶、窃密木马⁷、远程控制木马⁸、流量劫持木马⁹、下载者木马¹⁰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5：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6：网银木马是用于窃取用户网银、证券等账号的木马。

注7：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8：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9：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10：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。