网络信息安全周报

【2017】第 3 期

党委宣传部
信息网络中心　编

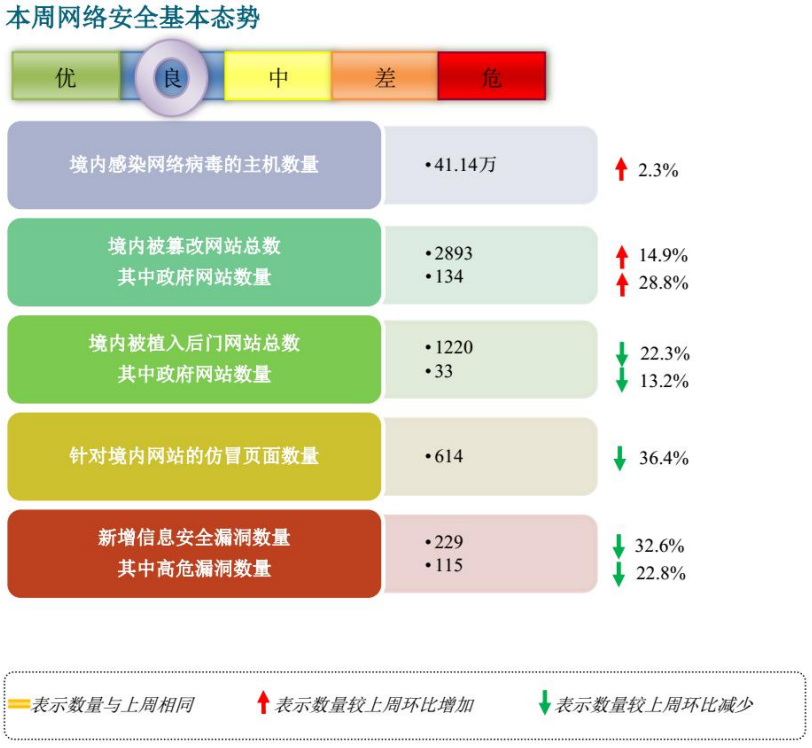
2017 年 3 月 16 日

本期要目

- 网络安全信息与动态（2017 年 2 月 27 日—3 月 5 日）
- 警惕“扫一扫”背后的诈骗陷阱
- 专家提醒：警惕熟人间以微信转账、发红包方式盗窃
- 关于办公 OA 系统无法打开 Word 文档等文件的处理办法

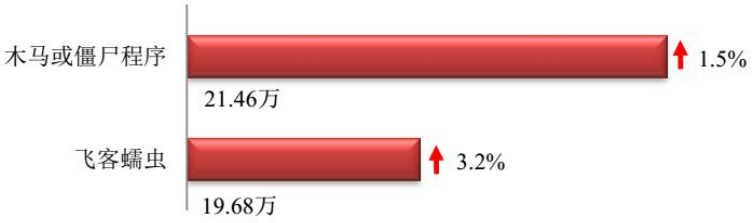
网络安全信息与动态（2017 年 2 月 27 日—3 月 5 日）

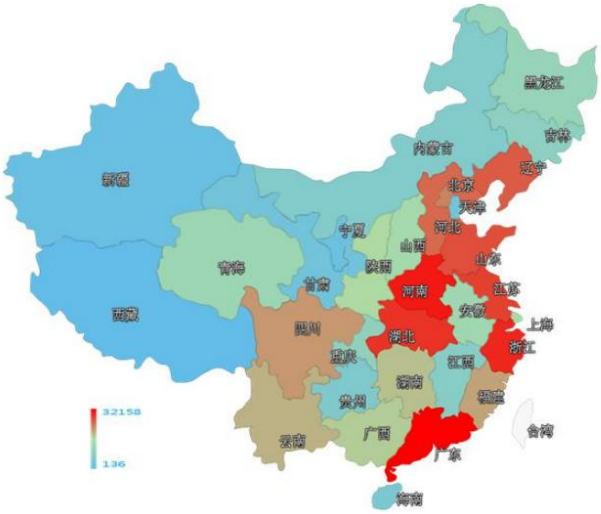
根据国家互联网应急中心最新公告数据：



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 41.14 万个，其中包括境内被木马或被僵尸程序控制的主机约 21.46 万以及境内感染飞客（conficker）蠕虫的主机约 19.68 万。

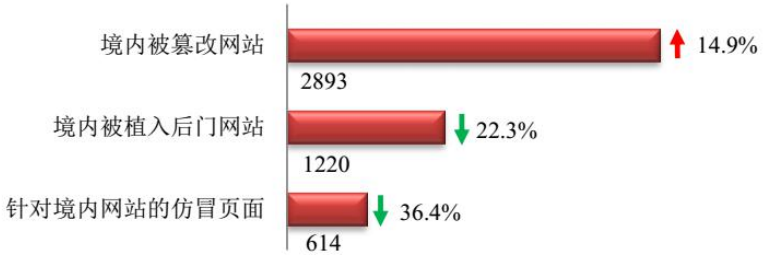




木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、河南省和浙江省。

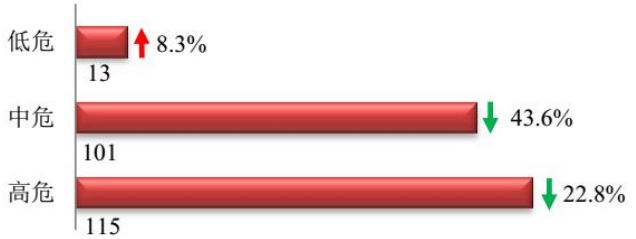
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2893 个；境内被植入后门的网站数量为 1220 个；针对境内网站的仿冒页面数量为 614。



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 229 个，信息安全漏洞威胁整体评价级别为中。



警惕“扫一扫”背后的诈骗陷阱

2017 年 02 月 28 日 19:48:49 来源： 新华社

日前，南京市民刘先生在扫描摩拜单车二维码时，出现了本不该出现的转账提示，于是向警方报案。当地有些市民也发现，扫描摩拜单车上的二维码后，如果不注意很可能钱就被转走了。

虚假二维码骗局并非孤例。在广东破获的一起二维码诈骗案中，犯罪分子通过扫码盗刷获利 90 余万元。

作为移动互联网的入口，二维码已被广泛应用于社交媒体、移动支付、产品促销、应用程序下载等方面。“新华视点”记者调查发现，由于制码技术几乎零门槛，不法分子将病毒、木马程序、扣费软件等植入二维码，消费者扫码被盗刷现象时有发生。

“扫一扫”背后的诈骗陷阱：覆盖正规码、木马植入、远程复制

针对消费者扫码遭诈骗，摩拜单车负责人称，单车上的正规二维码都是用钉子钉在车身上的，车费必须通过 APP 支付。车身上发现的二维码是后贴上去的，覆盖了原二维码，用户扫描的是不法分子的诈骗二维码。

在广东，佛山公安局禅城分局发现一起数十家店铺的收银柜台均被张贴虚假二维码案件。犯罪嫌疑人更换商家收款二维码，通过植入木马病毒的虚假二维码，获取消费者的手机信息和密码，进行网络盗刷。一共作案 320 余起，获利 90 余万元。

记者调查发现，除了用虚假二维码覆盖正规二维码实施诈骗，还有不法分子直接诱导用户扫描带有木马病毒的二维码。比如，浙江就多次发现不法分子以扫码得红包的形式诱导用户，一旦用户扫码后，手机会感染木马病毒，各种信息都被窃取了。

此外，有些不法分子通过拍照、截图、远程控制等方式获取用户付款二维码，盗刷用户银行卡。浙江台州微商赵女士就是一个受害人。在网络交易过程中，不法分子以自己支付宝余额不足为借口，提出让赵女士将付款码发给自己扫码付款。收到付款码截图后，不法分子随即进行复制，盗刷了赵女士的银行账户。

“付款码相当于银行卡加密码，不要轻易发给他人。”专家介绍，不法分子只要获取了，就可以进行复制，获取银行账户和密码。

“现在我都不敢随便扫码了，一不小心就可能被骗。可是现在生活中要用到二维码的地方又这么多，真是让人纠结。”杭州市民陈小姐说。

“以二维码作为入口的新型互联网诈骗案件层出不穷，一些不法分子将手机木马或恶意软件披上二维码的外衣在移动终端广泛传播。由于缺乏相关知识，没有防范警惕性，消费者个人很难防范。”浙江省网警总队有关负责人说。

专家称制码技术门槛几乎为零，骗子可轻易制“毒码”

业内人士介绍，二维码就是一张能存储信息的拥有特定格式的图形，能够在横向和纵向两个方位同时表达信息，能在有限的面积内表达大量信息。个人名片、网址、付款和收款信息等都可以通过二维码图案展现出来。

据了解，目前我国广泛使用的二维码为源于日本的快速响应码（QR 码），由于当时国内没有自主知识产权的二维码，市场几乎被 QR 码占据。QR 码没有在国内申请专利，采取了免费开放的市场策略。“这也意味着谁都可以通过网络下载二维码生成器。只需要将发布的内容粘贴到二维码生成器上，软件随即生成用户所需的二维码。”杭州某网络安全公司工程师郑孵说。

记者在网上搜索“二维码生成器”，发现了 205 万多个搜索结果，大部分的二维码生成软件可以直接在线使用。记者在首页选定了某一在线二维码生成平台，输入文字、图片、邮箱、网址后，瞬间就转换成了二维码。

“二维码的制作生成没有任何门槛。一些不法分子将病毒、木马程序、扣费软件等的下载地址编入二维码，用户一旦扫描，手机就会被植入的病毒木马感染，身份证、银行卡号、支付密码等私人信息就会被盗取。”阿里安全部资深品牌经理沈杰说。

“任何人都可以制作二维码，而且生成的二维码没有办法溯源，也没有相关的管理机构提供认证，这给警方侦破二维码诈骗案带来了很大困难。”浙江省网警总队工程师介绍。

建立回溯机制明确监管主体

郑孵介绍，目前，二维码的生产和流通并没有明确的主体进行统一的管理。虽然一些部门开始逐渐意识到二维码存在的巨大安全隐患，但还没有相关法律法规和具体举措。

“主管部门应该使用技术手段对二维码进行域名解析，通过设立专门的监管平台对二维码进行检测，过滤不良信息。”浙江工业大学计算机科学与技术学院陈铁明教授建议，“可以考虑建立二维码中心数据库，对市面上流通的二维码进行备案登记，将所有二维码数据统一存放在一个中心数据库，实现对二维码生成流通环节的有效追溯。”

“在管理层面上，有关部门应该对二维码的发布内容进行备案审查，对二维码的发布平台进行资质鉴定，对二维码的发布者进行实名登记，形成一整套完善的责任追溯机制。”陈铁明说。

浙江工业大学网络空间安全协会研究人员郑毓波认为，二维码使用企业应该加强相关的防护。据了解，目前微信和支付宝已经在软件里加强了安全监控保护，确保用户扫码安全。支付宝公司近日宣布，从2月20日起，支付宝付款码将专码专用，只用于线下付款。这就避免了一些不法分子利用二维码付款的机制实施转账诈骗。沈杰告诉记者，支付宝已经自带网址检测功能，用于判定扫描的二维码是否存在恶意链接。如果发现安全隐患，系统会发出安全提示，让用户判定是否需要进入跳转界面。

业内专家表示，用户也需要提高扫码安全意识。“不少人有不良的扫描习惯，看见二维码就扫，很容易落入不法分子的陷阱。”郑毓波说，应该加大知识普及，让大家了解二维码编码原理和二维码发布机制，不随意扫描来历不明的二维码，保护自己的信息安全。（记者：方列 参与采写：倪震洲）

（原标题：“扫一扫”钱就不见了？——二维码乱象调查）

专家提醒：警惕熟人间以微信转账、发红包方式盗窃

2017年02月10日 20:39:48 来源： 新华社

新华社北京2月10日电（记者熊琳）北京市通州区人民检察院近日发布由该院提起公诉的以微信转账、发红包方式盗窃他人账户钱款的案例。专家提醒，新兴盗窃形式呈现熟人作案、且犯罪多为临时起意等特点，被害人的防范意识有待加强。

2016年8月至11月间，赵某在其家中，使用闻某手机进行微信转账，分三次将闻某微信绑定的银行卡内的人民币49000元转到自己微信账户内。据了解，闻某是赵某母亲的好友，经常去赵某家，常向年轻的赵某请教如何使用网络购物。为网购方便，闻某告诉赵某其银行卡密码。赵某利用闻某信任，在闻某去其家中时操作闻某手机，用闻某手机微信绑定了闻某银行卡、设置支付密码，然后给自己微信账户转账，转账结束后即时解绑银行卡、删除记录，导致闻某几个月未曾发现钱款丢失。

经通州区人民检察院提起公诉，通州区人民法院判决赵某盗窃罪名成立。

通州区检察院审判监督部检察官助理汪玫瑰介绍，梳理案件特点发现，犯罪分子与被害人多为朋友、同事关系，有机会操控被害人手机，获取或修改被害人支付密码。作案时，犯罪分子多存侥幸心理，认为删除转账记录即可毁灭证据，不知移动支付方式转账留痕。此外，犯罪分子多为临时起意，赃款基本用于日常消费。

“随着新兴快捷支付方式的普遍应用，使用者的风险防范意识也应逐步提高。”汪玫瑰表示，为防范此类事件发生，建议使用者保护好支付密码，移动支付绑定银行卡里不存大额资金。手机丢失时及时关闭相关支付功能，不给犯罪分子可乘之机。

关于办公 OA 系统无法打开 Word 文档等文件的处理办法

当操作系统、浏览器、Office 软件或 WPS 软件等更新之后，在办公 OA 中打开文件附件时可能会提示文件无法打开，或者无提示一直无法打开文件的情况，一般处理过程是：

1.进入办公 OA 主页（地址为：219.246.21.180），不登录系统，单击“登录”按钮下的“[辅助程序安装]”链接，如下图所示：

2.系统弹出“自动安装和更新”窗口，此时应关闭浏览器窗口，然后选择相关软件进行安装和更新即可。如果自己无法确定选择哪些程序，可以全部“重新安装”，即选择“全选”选框，并单击“更新全部已选插件”按钮。

3.关闭“自动安装与更新”窗口，重新启动浏览器并登录即可。

抄送：校领导