网络信息安全周报

【2017】第 2 期

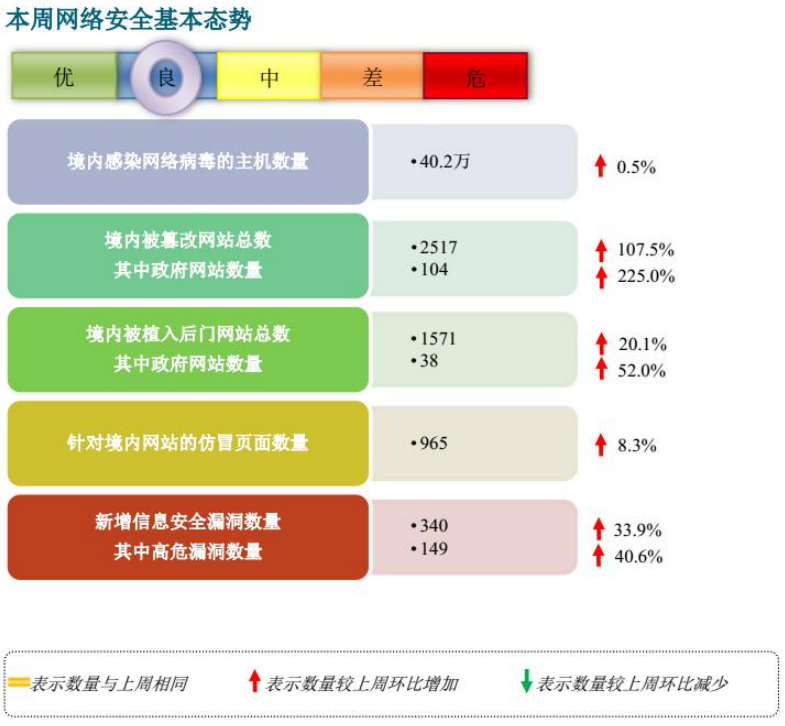
党委宣传部
信息网络中心　编　　2017 年 3 月 9 日

本期要目

- 网络安全信息与动态（2017 年 2 月 20 日—2 月 26 日）
- 工信部：未经批准不得自行建立或租用 VPN
- 基于物联网、智能化恶意软件和勒索软件的攻击将成为 2017 年主要威胁活动

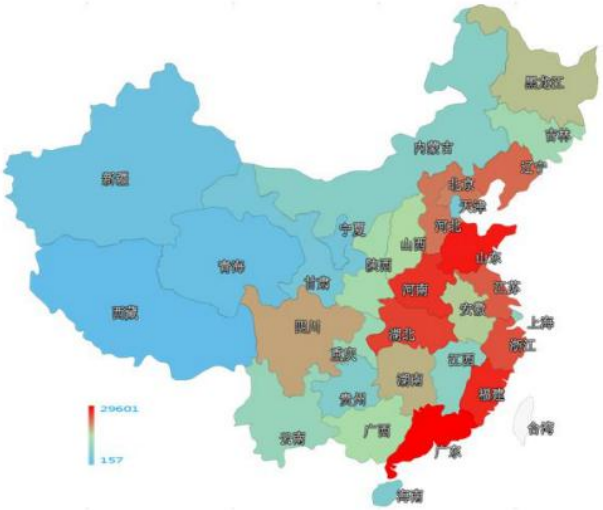
网络安全信息与动态（2017 年 2 月 20 日—2 月 26 日）

根据国家互联网应急中心最新公告数据：



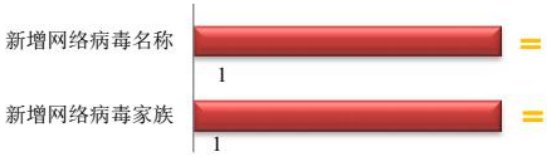
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 40.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 21.1 万以及境内感染飞客（conficker）蠕虫的主机约 19.1 万。



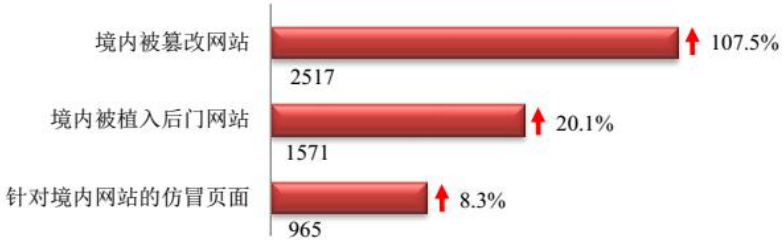
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、山东省和福建省。

本周 CNCERT 捕获的新增网络病毒文件，按网络病毒名称统计新增 1 个，按网络病毒家族统计新增 1 个。



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 2517 个；境内被植入后门的网站数量为 1571 个；针对境内网站的仿冒页面数量为 965。



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 340 个，信息安全漏洞威胁整体评价级别为高。

工信部：未经批准不得自行建立或租用 VPN

2017-01-25　来源：腾讯网

腾讯网 1 月 22 日消息 1 月 22 日从工信部网站获悉，工信部决定自即日起至 2018 年 3 月 31 日，在全国范围内对互联网网络接入服务市场开展清理规范工作。

工信部将依法查处互联网数据中心(IDC)业务、互联网接入服务(ISP)业务和内容分发网络(CDN)业务市场存在的无证经营、超范围经营、“层层转租”等违法行为，切实落实企业主体责任，加强经营许可和接入资源的管理，强化网络信息安全管理，维护公平有序的市场秩序，促进行业健康发展。

通知提出，各通信管理局要对本辖区内提供 IDC、ISP、CDN 业务的企业情况进行摸底调查，杜绝无证经营、超地域范围经营、超业务范围经营、转租转让经营许可证等非法经营行为。各基础电信企业、互联网网络接入服务企业要全面自查，未经电信主管部门批准，不得自行建立或租用专线(含虚拟专用网络 VPN)等其他信道开展跨境经营活动。

基于物联网、智能化恶意软件和勒索软件的攻击将成为 2017 年主要威胁活动

来源：ZD 至顶网安全频道　2016 年 12 月 13 日

前不久，犯罪分子劫持了物联网设备，并用来对某 DNS 解析服务基础设施发起大规模 DDoS 攻击，使得大部分互联网服务停止运行；犯罪分子试图运用窃取

的文档影响美国总统大选；勒索软件活动开始变得猖狂，包括针对高价值目标的勒索案例。这些勒索活动和类似攻击对受害者产生了极大影响。

基于物联网、智能化恶意软件和勒索软件的攻击将成为2017年主要威胁活动

通过研究过去一年中网络威胁的变化，一些趋势变得明朗：

• 企业和个人数字化足迹的急剧扩大，增加了潜在受攻击面。

• 一切皆可成为目标，任何信息均可能被用于攻击的突破口。

• 威胁正变得日益智能化，可独立运行，增加了检测难度。

• 我们看到两种威胁趋势：针对成群小型目标进行自动攻击，以及瞄准大型目标进行的针对性攻击。这两种趋势的混合程度越来越高，第一阶段使用自动攻击，第二阶段采用针对性攻击。

基于这些趋势，FortiGuard全球威胁研究与响应实验室对2017年网络威胁的发展趋势进行六种预测：

1.物联网设备制造商将需要为安全漏洞负责

我们正处于围绕物联网的“完美风暴”中：预计联网设备将在2020年增长到200亿以上的数量级，这是一个巨大的M2M（机器对机器）攻击面；这些设备使用高度脆弱的代码，由不同的供应商提供，几乎没有任何安全战略。当然，这些设备大部分是无脑设备，意味着我们不能添加安全客户端或有效更新其软件或固件。

现在，攻击者可以运用很多手段成功利用已知证书，比如默认用户名和密码，或者硬编码后门。此外，物联网设备中还有一些几乎“唾手可得”的漏洞，包括编码错误、后门和其他垃圾代码（通常用于启用物联网连接和通信）引起的缺陷。考虑到破坏和收益的潜在可能，我们预测瞄准物联网设备的攻击将变得更复杂，更多经过设计的可利用物联网通信和数据收集链中的漏洞将涌现出来。

一种可能的发展是影子网络或物联网僵尸网络的崛起，这些网络不能用传统工具进行探测或测量。影子网络攻击开始时采用针对性分布式拒绝服务（DDoS）攻击与勒索需求相结合的方式。随后可能采取收集数据、针对性攻击、混淆其他攻击等方式。

围绕物联网设备的安全话题越来越沉重，已经到了政府部门无法忽视的程度。我们预测：除非物联网设备制造商采取紧急行动，否则他们将不仅遭受经济损失，还会因为其产品中的安全漏洞而成为法律诉讼的对象。

2.从智能到更加智能：需要针对拟人攻击实施更智能的防护措施

大部分恶意软件是不会说话的——仅仅针对特定目标进行编程。黑客仅仅将其指向一个目标，该恶意软件或者完成任务，或者不能完成任务。网络罪犯采取两种方式补偿此类恶意软件的二元本质：通过对多种工具进行时间密集型管理将攻击引向特定目标，或者通过规模进行补偿。传播足够的恶意软件，或者让恶意软件自我复制足够的次数，最终找到途径进入可以利用的设备内部。

这种情况即将改变。

威胁正变得更加智能，逐渐能够独立自主地运行。我们有望在来年看到具有自适应功能的恶意软件，通过学习成功经验以提高攻击的成功率和有效性。这种新一代恶意软件将具有环境感知能力，能够理解其所处环境并准确决定下一步的动作。自主恶意软件在很多方面表现得像人类攻击者：目标侦察、识别目标、选择攻击方式、智能规避检测。

3.200 亿物联网和终端设备是云端攻击时最薄弱的环节

向云计算、云存储、云处理、甚至云端基础设施的迁移正在加速。访问云资源的远程设备多达数百万，使这种 IT 服务提供模式易于受到黑客攻击。

云安全在于控制网络访问者并了解其中有多少是可以信任的。我们有望在下一年看到精心设计的攻击利用终端设备并破坏这种信任模型，从而在客户端侧发起针对云服务供应商的有效攻击。

4.攻击者将集中攻击智慧城市

越来越多的国家正在构建智慧城市。关键基础设施的互联性、应急服务、交通控制、物联网设备（比如自动驾驶汽车）、以及投票、付账、商品和服务配送等将形成巨大的攻击面。这些集成系统受到大规模破坏的可能性很高，是黑客眼中极具价值的攻击目标。

我们预测黑客会将目标转向楼宇自动化和楼宇管理系统。就像物联网分布式拒绝服务（DDoS）攻击那样，这些攻击可能首先采取粗糙鲁莽的攻击方式，比如仅仅关闭楼宇的系统。但是很有可能会通过锁死房门、关掉电梯、改变交通路线或打开报警系统等方式劫持楼宇进行勒索。一旦发生这种情况，黑客很可能会控制部署在智慧城市各处的集中式系统。

5.勒索软件只是入门级恶意软件

由于有利可图，勒索软件即服务（RaaS）在 2016 年的增长势头很可能会延续到 2017 年。我们同样会看到以下基于勒索软件的攻击活动即将来临：

针对性攻击的成本更高

我们有望看到对备受瞩目的目标发起的极具针对性的攻击，比如社会名流、政治人物和大型组织。除锁定系统外，这些攻击者可能还会收集敏感或个人数据以用于勒索或讹诈。

自动化攻击和物联网勒索活动

以普通公民和消费者为目标存在一个成本阈值，使攻击者通常难以控制成本收益。个人会支付多少赎金以解锁其硬盘、汽车或关闭防火警报？我们预测这种限制将在 2017 年得到解决，因为自动化攻击将规模效益引入勒索软件，使黑客能够以较低代价从大量的受害者那里同时榨取小额金钱，特别是瞄准在线物联网设备。

继续瞄准医疗卫生行业

被窃取的患者记录的勒索价值在于其替代能力患者记录和其他人员数据比信用卡更难以替代。这些记录也具有很高的价值，因其可用于欺诈。

除非医疗卫生机构实施严格的安全措施，我们预测该行业中的很多单位将成为勒索攻击的目标。其他需要收集并管理人员数据的行业，比如律师行、金融机构和政府部门，将会遭受更多攻击。

6.必须研发能够解决关键网络技能人才短缺问题的技术

目前技术精湛的网络安全人才短缺状况意味着很多公司在参与数字经济时将承担很大的风险。它们不具备必要的经验以研发安全策略、保护在网络环境中移动的关键资产、或者识别如今复杂的网络攻击并作出响应。

很多公司的第一反应是购买传统安全工具，比如防火墙或 IPS（入侵防护系统）设备。但是管理这些设备需要专门的资源，而且这些工具越来越难以为如今使用的高度动态的、广泛分布的网络提供有效的安全防护。

我们预测那些聪明的公司将会转而求助于可以带领它们走出安全迷宫的安全咨询服务机构，或者是可以提供一揽子解决方案的管理安全服务供应商。这些公司还会将大部分基础设施迁移到云端，从而只需点击鼠标就可以添加安全服务。

抄送：校领导