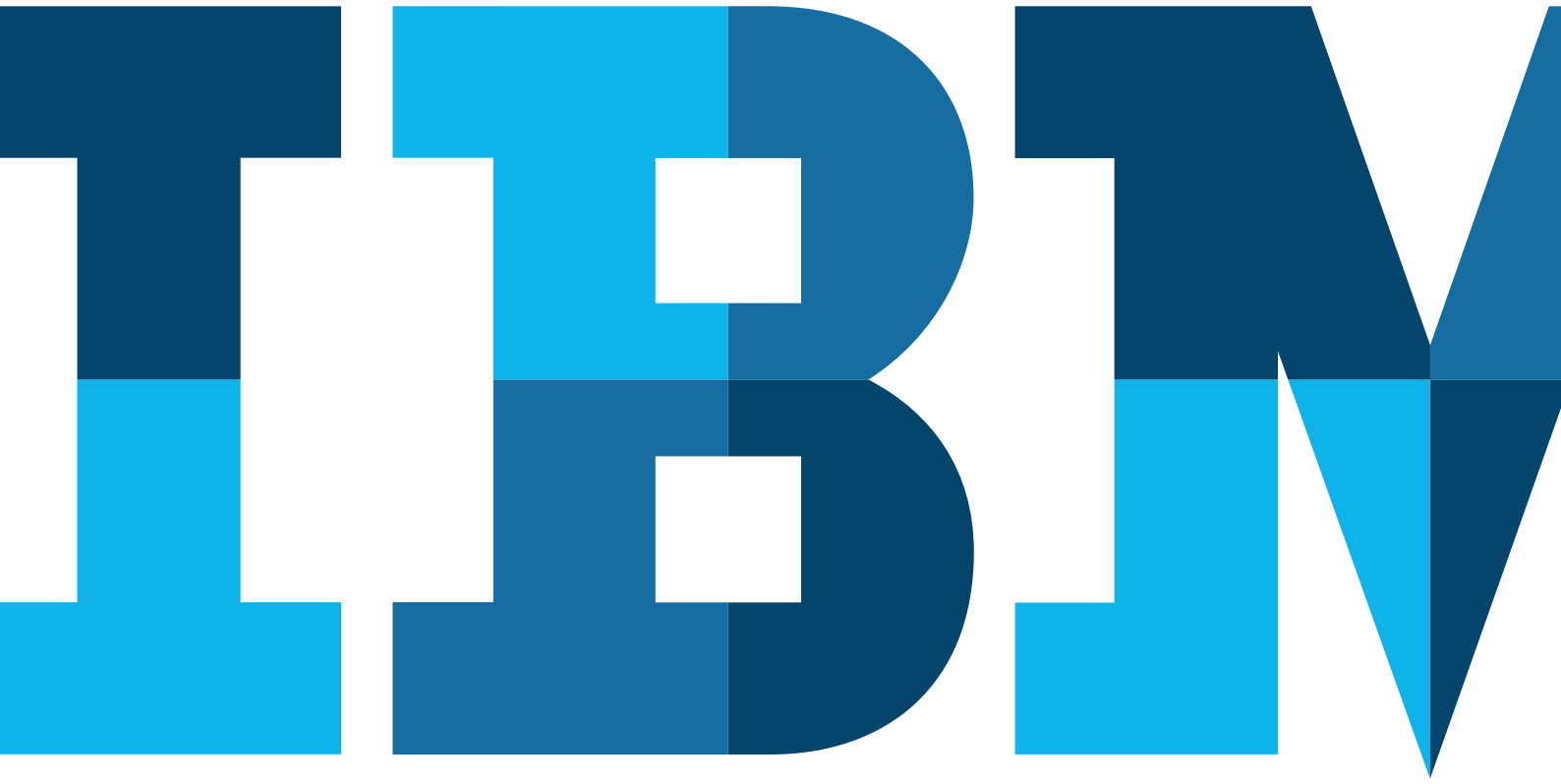
IBM X-Force威胁情报季度报告
2014年第四季度

近距离观察当前的网络安全风险——从物联网新威胁到恶意软件和僵尸网络的感染源



IBM

目录

摘要

随着年末临近，IBM® X-Force®研究与开发团队再度发布全球安全趋势研究报告。报告特别分析了由于互联网连接的人、地点和事物越来越多而导致的一系列新安全风险。

首先，我们来看物联网的安全。如今，从恒温器、汽车到医疗设备，我们生活中各种“事物”的普遍连接意味着在硬件制造商开发最先进技术的同时还伴随着软件开发。安全行业可从一开始就帮助制定针对嵌入式软件的安全实践。这不仅可以创造安全软件的新时代，还可大量减少影响物联网安全的违规事件。

在2014年11月的一份报告中，分析师估计物联网连接的 “事物”将从2013年的99亿增加到2020年的300亿。这些相互连接的“事物”大多由收集和传输数据的智能系统驱动[1]。随着这些事物被制造和销售给消费者，该连接性正在改变我们的生活方式，并带来有关个人隐私、市场营销和互联网安全的新问题。

意图控制数据、身份和密码的不良行为者从未放弃研究和利用那些安全性不高的联网设备，因此这些设备比PC、笔记本电脑或平板电脑更易成为受攻击目标。对于使用这些新生技术的企业和员工而言，在连接到企业安全区时，充分考虑其伴随而来的风险在现在变得非常重要。我们将在本报告稍后讨论有关个体风险，以及在这些重要领域有帮助作用的保护措施。

其次，我们关注地点，具体而言主要是互联网上不安全的地点。借助我们的包含超过230亿个URL和IP地址的数据库，我们分析了哪些国家的恶意软件和僵尸网络感染比例最高，及其在过去14个月的形势变化。

和每一次的IBM X-Force威胁情报季度报告一样，人同样是关注的中心。作为安全从业者，我们希望对安全的事物和地点安全的洞察有助于保护您自己的网络。我们还会在2015年进行年底总结，回顾2014年的安全趋势并展望下一年的情况。

保护物联网新世界的安全

从联网的汽车到可编程心脏起搏器，在普遍连接的世界中如何才能保证敏感数据的安全和可靠？

您的下一个移动设备可能是真正移动的——带有轮子和仪表盘。如果您有现代心脏起搏器或胰岛素泵，您将不仅是联网器械的使用者，还将是宿主。最新趋势是将一切具有计算能力的东西都连接到互联网，包括汽车、可植入医疗器械和智能电表。甚至像家电[2]、牙刷[3]和饮水杯[4]等传统上未计算机化的物体，现在也在物联化和连接。

这一波物联化和连接称为物联网（IOT）。像云和移动等别的广泛技术类别一样，物联网也能提供生产力和生活质量改善，不过也伴随着许多未知的安全威胁。

过去几年，这一无处不在的连接性已在 黑帽（Black Hat）和DEF CON等安全大会上受到关注。2011年，一位安全研究人员演示了如何“黑进”自己的胰岛素泵，前提是只需要知道设备的序列号[5]。再最近，有两位研究人员公布了他们关于联网汽车安全的发现，包括在一档美国早间脱口秀节目上演示如何控制两种品牌的汽车[6]。

像大多数新技术的称呼一样，“物联网”的含义也相当含糊。物联网究竟由什么组成？我们大多数人会想到家庭自动化功能，如Google Nest——由恒温箱和烟雾检测器连接而成的网络。联网的汽车也包含在物联网中。但具有“事物”访问功能的智能手机和平板电脑该怎么算？这些设备也是“事物”吗？

大型机、服务器、工作站和便捷式电脑等传统计算设备该怎么算？它们是完备的“事物”还是只是旧的“计算机”？它们没有那么新，给它们贴上诸如物联网这样的前沿标签似乎也不合适。另外还有工业控制和监控及数据采集（SCADA）系统。其中有些系统如此陈旧（许多都嵌入地板水泥底下，早在上世纪50年代就埋在那里了），以致它们本身并不支持IP连接，但可以通过IP网关接入互联网。

显而易见，物联网是一个实际上对安全专业人员没有意义的概括性术语：构成广阔物联网的设备执行各种功能，伴随着差异极大的威胁，需要有针对每一类设备的安全策略。IBM建立了一个物联网模型，对理解各种数据流和控制过渡点的安全威胁很有帮助。该广义模型可容纳所有类别的“事物”，但并非所有“事物”都需要该模型的所有要素。

所有“事物”先连接到局域网，然后再连接到全局网——通常是互联网。传统计算机和基础设施设备就是如此。大型机、服务器、台式电脑、便捷式电脑、路由器和交换机全都连接到局域网（服务提供商设备可能直接连接到互联网），并路由至互联网（高度机密的政府网络除外）。工业控制系统可能是隔离的。

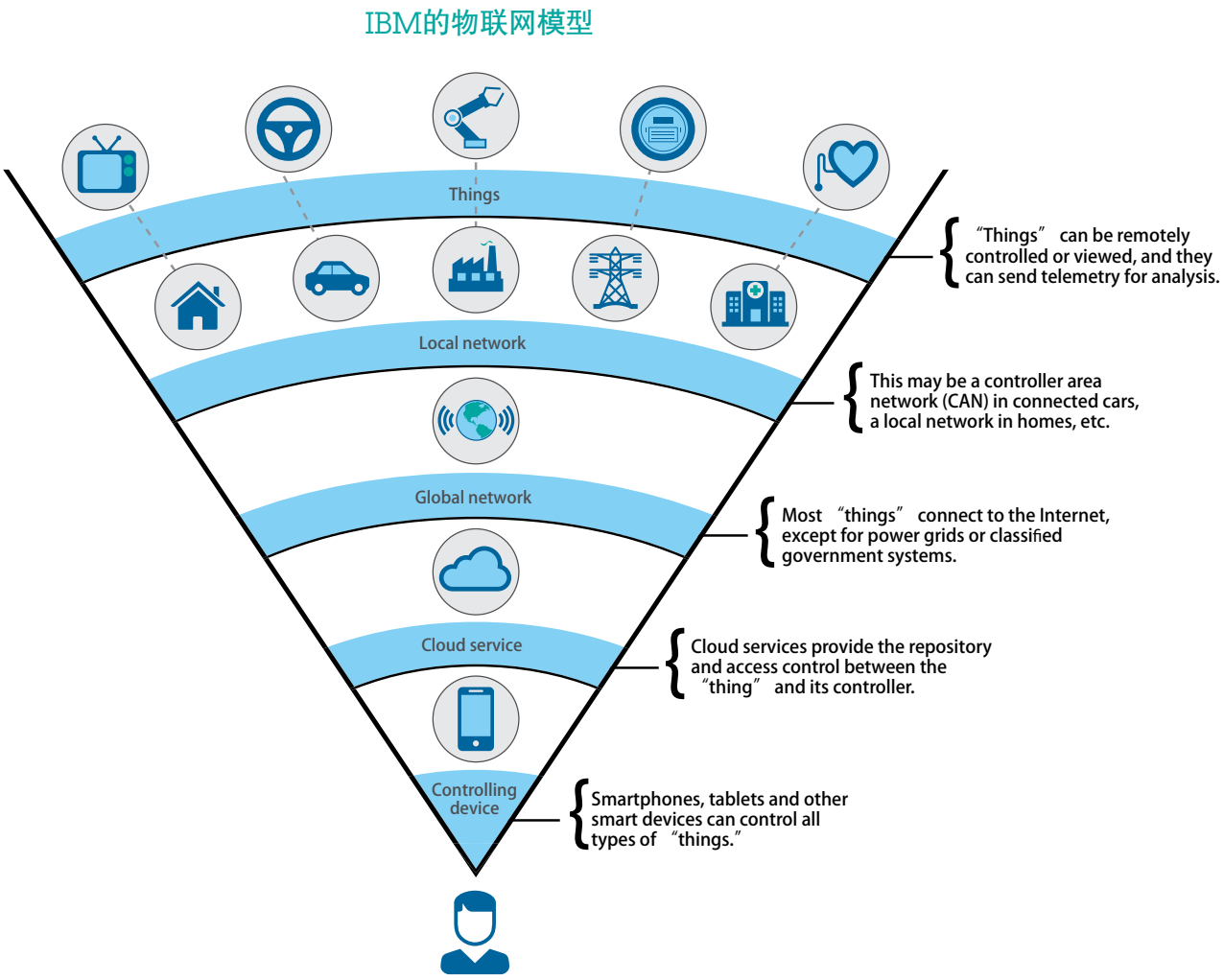


图 1. IBM物联网模型

也许"事物"的最典型特征是以远程方式 (常常是从智能移动设备) 查看和控制它的能力。"事物"还能向中央心仪和分析点发送遥测信号。云服务常常在"事物"及其控制器之间提供信息存储库和访问控制。

我们来分析几个"事物"，来看一看它们是如何适应该模型的。

家庭自动化

该类别可能包括智能家电，如冰箱（报告其温度并在没有西兰花时提醒您）、照明和音响系统、电视、恒温箱和烟雾检测器、警报系统、车库门，甚至门锁。这些“事物”连接到家中的局域网（常常是无线网），局域网通常通过服务提供商经由入户光纤或宽带电缆连接至互联网。安全系统可能还有辅助连接（使用移动网络）。

服务提供商或公共事业公司可能提供家庭自动化服务，例如AT&T Digital Life services或Consumers Energy EnerLink.Net[7]。作为选择，业余爱好者可构建自己的家庭自动化解决方案并绕过云层，直接从移动设备或传统计算机连接到其家庭局域网。

联网汽车

对于联网汽车，局域网可能是控制局域网(CAN)，您的制动器、发动机、电动车窗和其他部件的电子控制单元（ECU）就是连接到控制局域网。全局网是您的移动载波商，云服务常常是汽车制造商的网络，汽车要通过该服务识别自己的身份，您也要通过自己手机上的应用程序进行身份认证。

联网汽车有许多功能，除了紧急呼叫外，通过基于订阅的诊断系统，汽车能够报告遥测数据，如速度、位置和发动机温度。您能够用自己手机上的应用程序监控您的汽车，以远程方式启动，按照天气情况将驾驶舱的温度调节到最好，并看着它达到理想温度。制造商或服务合作伙伴能够分析来自电子控制单元的遥测数据，以预测故障，甚至从ECU分析遥测数据，以预测故障，甚至在智能手机日历与汽车同步时安排预约维修时间。

工业控制和SCADA系统

工业控制和SCADA系统因行业、使用年限和用途不同而差异很大。例如，蔗糖加工厂的系统可能较老，只通过一个串行端口报告机器的状态和接受控制命令。系统控制由操作员控制台（可能与IT网络的其他部门分开）通过拨号线路进行控制，没有互联网连接或从工厂外部网络控制SCADA系统的能力。相比之下，较新的工业控制系统基于Windows和Linux等通用操作系统，可连接到IP网络。

智能电表

智能电表正在推动操作技术（如前面讨论的工业控制和SCADA设备）与传统IT网络的融合，这是因为经过分析的遥测数据被提供给计费系统，并且常常可通过网站提供给顾客。最终，顾客将能通过使用其手机连接能源提供商的云环境来选择其电能来源，例如由具有太阳能电池板的邻居组成的微型电网。

顾客还能选择在凌晨两点钟运行其洗碗机，其能源仪表板上的信息会通知他们这时使用家庭自动化和智能能源的电费最便宜。更好的是，您将能够设置过滤条件，以允许洗碗机和能源提供商根据实时能源价格协商在何时清洗碟子。

可植入医疗器件

现代可植入医疗器械可将遥测数据提供给医生，使医生能够监测器械的性能和进行调整。这是通过无线电方式连接到专用控制设备来实现的，距离比较有限。但是，医疗行业的转变要求患者通过患者网站获取其数据，要求整个医疗服务提供商和保险商生态系统可获取统一的患者护理信息。实现下面的场景并不困难：心脏起搏器将其状态报告给医生，医生通过互联网对起搏器进行调整，这可能是通过航班无线服务，从而在国外航班飞行途中挽救患者的生命。

对“事物”的威胁已经存在

研究人员修改了车载通信系统单元的固件，使他们能访问所有车载电子控制单元。于是他们在车速40英里/小时情况下成功禁用了汽车的制动功能。该攻击是通过播放一张专门制作的包含MP3的CD来进行的，在CD正常播放时，利用播放器软件的缓冲区溢出漏洞进行攻击[8]。

某产品制造商想提供对包括暖通空调和安防控制在内的楼宇系统的远程访问，该功能内建了一个后门管理账户。该账户提供无密码访问，可用于获取对至少一个业务的未授权访问：显示“办公室的平面布置图，包括针对每个办公和工厂区域的控制手段和反馈。”该系统被超过16,000个企业使用，暴露在互联网中，中间没有部署防火墙[9]。

薄弱的加密方案不仅留下了可通过网络连接的照明漏洞，使其容易被利用，而且暴露了他们的Wi-Fi网络连接密码。尽管使用的是美国国家标准与技术协会（NIST）的高级加密标准（AES），但照明设备仍然可使用从未变更的预共享密钥通过网络相互通信[10]。

“事物”需要什么

简言之，虽然“事物”可能各种各样并需要不同的安全控制（您是否真的想在您的起搏器上运行防病毒软件），我们的模型有助于定义保护点和每个保护点应当实施的安全控制的类型。例如，“事物”需要：

- **带有可信赖固件保证的安全操作系统。**这包括通过不可信赖的连接进行网上/无线电更新的能力。
- **唯一标识符：**虽然IPv6是识别网络上“事物”的关键，但“事物”也需要订用可信赖的身份数据库：因为许多“事物”并不直接与用户（如传统计算机）互动，所以传统身份认证的概念并不适用（硬编码管理凭证[11]不是可接受解决方案）。特别是在“事物”在机器对机器（M2M）环境（如汽车CAN）中互动时，每个“事物”必须能够信赖其他“事物”。
- **强大的身份认证和访问控制。**当用户访问有关“事物”的数据或控制“事物”时（通常通过来自用户移动设备的云服务），关键是确保用户是其本人。您肯定不想让小偷用简单的用户名和密码解锁和启动您的汽车，特别是考虑到最近的凭证危害[12]暴发和大多数用户选择简单密码的事实。实际上，研究显示，“123456”和“password”仍然是互联网上最常见的两个密码[13]。
- **数据隐私保护。**流向“事物”和从“事物”流出的数据——以及可能存储在“事物”或其控制设备上的数据——常常都是敏感数据。驾驶员可将其手机连接到车载信息娱乐系统，该系统能够访问其联系人信息并有可能访问其电子邮件和短信。随着移动支付开始出现在新手机上，通过车载系统还有可能访问信用卡信息。如果保护不当，用于访问家庭自动化和和工业控制系统的凭证也可能泄露。隐私问题的解决方案常常是数据及传输加密。
- **强大的应用安全性。**安全漏洞起因于软件错误（bug）。硬件制造商常常并不擅长软件开发，包括可驻留在“事物”上或者作为云门户和移动应用程序形式存在的Web应用程序。在软件界内部，安全漏洞数量庞大且常常是灾难性的，就像最近的 Heartbleed OpenSSL 漏洞[14]和更近的 Bash Shellshock漏洞[15]。“事物”制造商每天都在提出新的产品想法，但可能不实施安全开发生命周期或者不开展彻底的安全和功能试验就匆忙将其产品推向市场。

IBM物联网模型仍在发展之中，因为作为整体的物联网仍在发展演变，其中蕴含着风险和机遇。

这是“事物”革命的开始，像移动设备一样，“事物”的制造商和开发商也可帮助推动在安全方面的必要行动，而且从一开始就进行，而不是在事后进行轻率的变动。但与移动设备市场不同的是，物联网制造市场广阔得多，不像前者那样只有一小撮硬件制造商和更少的移动运营系统。许多物联网“事物”的制造商是新成立的小企业，因而没有资金或资源来将安全添加到其设计和开发预算及时间表上。除了资源短缺，还有一些其他挑战：

- 传统软件市场在代码可靠性上的表现并不出色。SQL注入攻击仍是一个巨大问题的事实表明，我们在对开发人员以及作为整体的行业进行的关于在开发和生产环境下可靠地编码和测试应用程序的培训方面并未取得很大的进展。
- 负责制造“事物”的硬件制造商通常并不擅长软件开发。如同前面提到的，许多软件公司在编写可靠代码方面也做得并不好。
- 实施和配置系统、软件及“事物”的任务落在最终用户的肩上，在企业中就是IT部门。消费者并不总是想到安全性，即使在想到时，找到或理解有关物联网的安全设置也并不容易。此外，一些应用程序需要广泛（和不可靠）的设置才能正常工作。虽然“事物”常常是作为消费商品开始，但它们会演变成企业“事物”——就像移动技术一样。但大多数 IT 部门并不负责管理这些“事物”的物理安全，这可能预示着企业内部安全管理的所有方面的整体转变。
- 许多“事物”最终将需要IPv6地址，这带来了许多安全威胁。许多系统和网络管理员都没有很好地理解IPv6，更不用说那些需要对其有线调制解调器进行IPv6配置的家庭用户了。要使一种技术具有安全性，您首先需要是其工作原理方面的专家。我们有一整期X-Force威胁情报季度报告会关注IPv6安全性，包括用它来防范高级分布式拒绝服务攻击（DDoS）、隧道式穿越防火墙以及入侵和异常检测的可能性。这些只是我们知道的一些威胁。
- “事物”依赖种类非常多样的协议集，如MQTT、XMPP、DDS、AMQP、Zigbee和Z-Wave，和一些过去遗留的工业协议，如Modbus和DNP3，以及新的汽车协议，如车对车（V2V）和基础设施对车（I2V）通信协议。其中每个协议都有各自的安全挑战。

为帮助克服物联网内部的安全挑战，IBM X-Force建议制造商：

- 遵循开放式Web应用安全项目（OWASP）物联网十大规范[16]
- 构建可靠的设计和开发规范
- 对产品进行定期渗透测试
- 遵循行业指引，如IBM汽车安全观[17]

技术还能帮助通过接受物联网来提高安全性，但需要有批判性的眼光。您可以成为早期采用者，而不是受害者。购买酷的设备，但不要盲目投产。要在模拟环境中对产品进行安全测试；然后与厂家合作，帮助他们理解缺点和给予纠正。如果厂商没有反应，则遵循负责任的漏洞披露指导方针，如标有CERT[18]和X-Forc[19]团队公布的内容。齐心协力，我们就能帮助确保物联网发展成为更安全、更可靠的场所。

声誉值：恶意软件和僵尸网络的源头

通过我们的IP声誉数据库了解哪些国家是恶意软件和僵尸网络感染的活跃源头。

IBM X-Force研究人员持续跟踪包含恶意软件的网站，并将信息存储在我们的IP声誉数据库中，IBM客户可使用该数据库来帮助保护其网络。这些网站可能就是为托管恶意软件而建立的，或者是受到破坏或毒害的合法网站。我们的数据库还包含“匿名”服务使用的IP地址，这些地址经常用于发送垃圾邮件。

最近，随着诸如Heartbleed（心脏出血）和Shellshock（破壳）等普遍性漏洞的披露，X-Force想建立大规模分发恶意软件来源的基线。根据我们的研究，报告的这部分内容分析了恶意软件链接最常托管于哪些国家，以及僵尸网络指令和控制（C&C）服务器的地理分布。我们还将当前情况与过去14个月的数据做了比较。

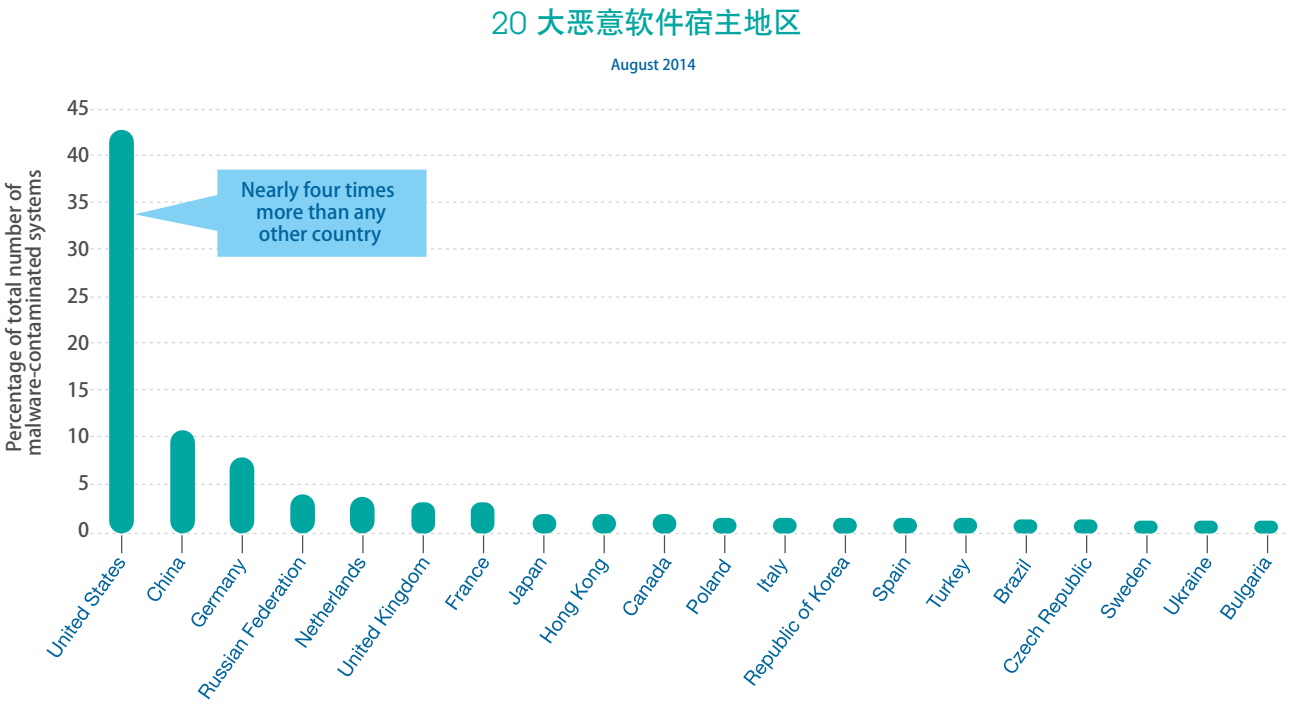


图 1. 20 大恶意软件宿主地区，2014 年 8 月

对于排在前列的托管恶意软件的国家，图1显示：

- 以美国为主，托管的恶意软件链接占全部数量的43%。
- 恶意软件的第二大集中地是中国，为11%。（有意思的是，这是前一年的两倍）。
- 德国从第二下降排在第三，目前为8.3（比14个月前下降了9.8%。）
- 排名第四至第七的接下来四个国家的名次与2013年没有变化 。来自这些国家的恶意链接数量非常相似：俄罗斯联邦、荷兰、英国和法国都在3.6 - 3.3%之间。

在僵尸网络C&C服务器的地理分布方面，图示是相似的。图2显示：

- 来自美国的服务器数量多于其他任何国家，占受感染系统总数的四分之一。但十四个月前这个数字还比现在多4%。
- 具有第二多C&C服务器的国家是俄罗斯联邦，约为9%。

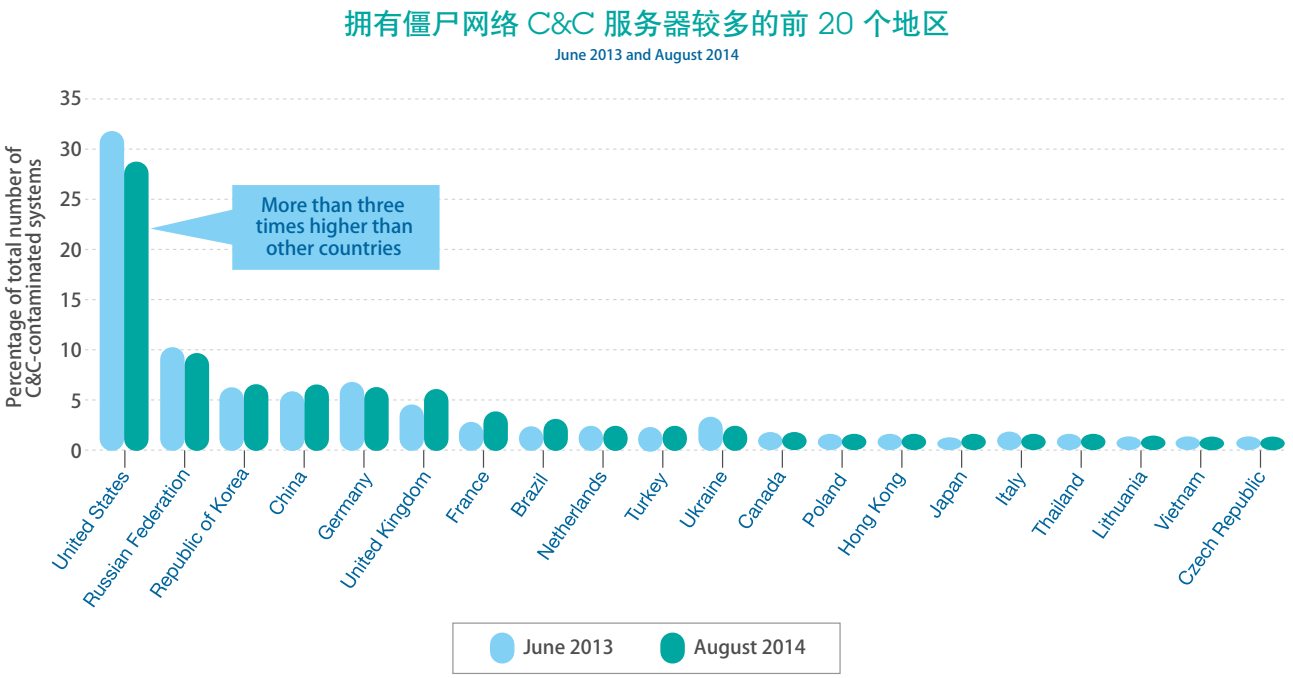


图 2. 拥有僵尸网络 C&C 服务器较多的前 20 个地区，2013 年 6 月与 2014 年 8 月

供图: Team Cymru

- 韩国、中国、德国和英国比较相近，拥有C&C服务器的比例在7.2 - 6%之间。

如图1和图2所示，技术用户和服务提供商数目越多的国家的排名越靠前，这并不令人奇怪。因此，我们决定根据IP地址与对应国家的IP可寻址系统总数之比对图中数字进行标准化。

图3显示，当对数据进行标准化之后，美国不再在托管恶意软件较多的前20个国家中，而是下降到25位。香港、立陶宛和保加利亚现在出现在排在前三位。而立陶宛的受恶意软件感染的系统百

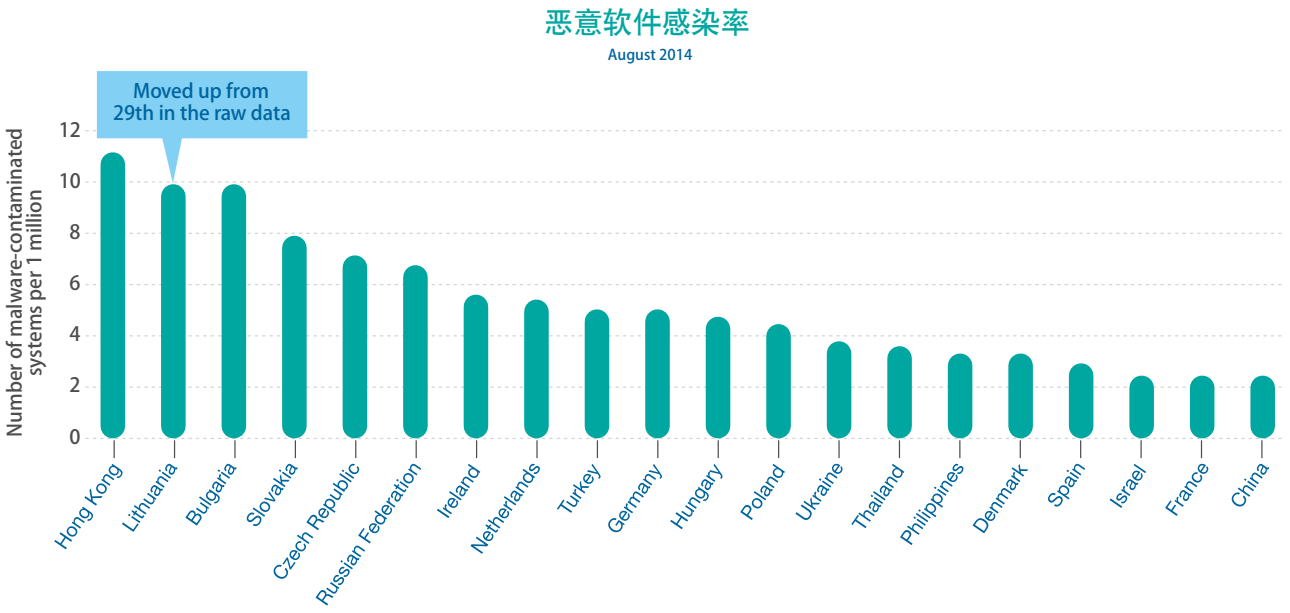


图 3. 恶意软件感染率（感染系统占全国系统总数的百分比）， 2014 年 8 月

分比可能并不领先，图4显示其 C&C 服务器感染数量领先。

在对C&C服务器感染数据进行了标准化后，图4显示美国不再在C&C服务器较多的前20个国家之中，下降到28位。俄罗斯联邦人第二位移到第三位。立陶宛大幅响跃升到首位，白俄罗斯、斯洛伐克、乌克兰、土耳其、泰国、香港、匈牙利、捷克共和国和波兰全都高于平均值（亦即每百万个系统有略少于2个系统受感染。）

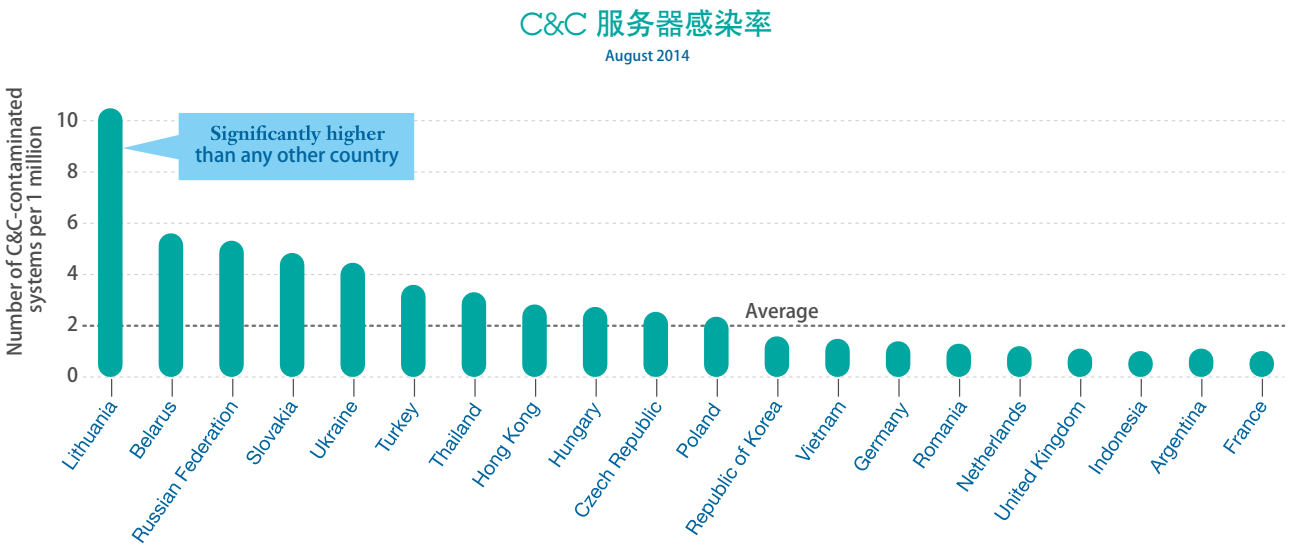


图 4. C&C 服务器感染率（受感染系统占全国系统总数的百分比），2014 年 8 月

比较2013和2014年的数据可以看出，除立陶宛以外，几乎所有国家的受感染C&C服务器总数都下降了，立陶宛是不仅在2014年排在首位，而且受感染系统比率增加了一个系统（每百万个系统）。斯洛伐克的数字年比持平，印度尼西亚有所增加。有意思的是，乌克兰的感染率大幅下降，减少了约5个系统（每百万个系统）。

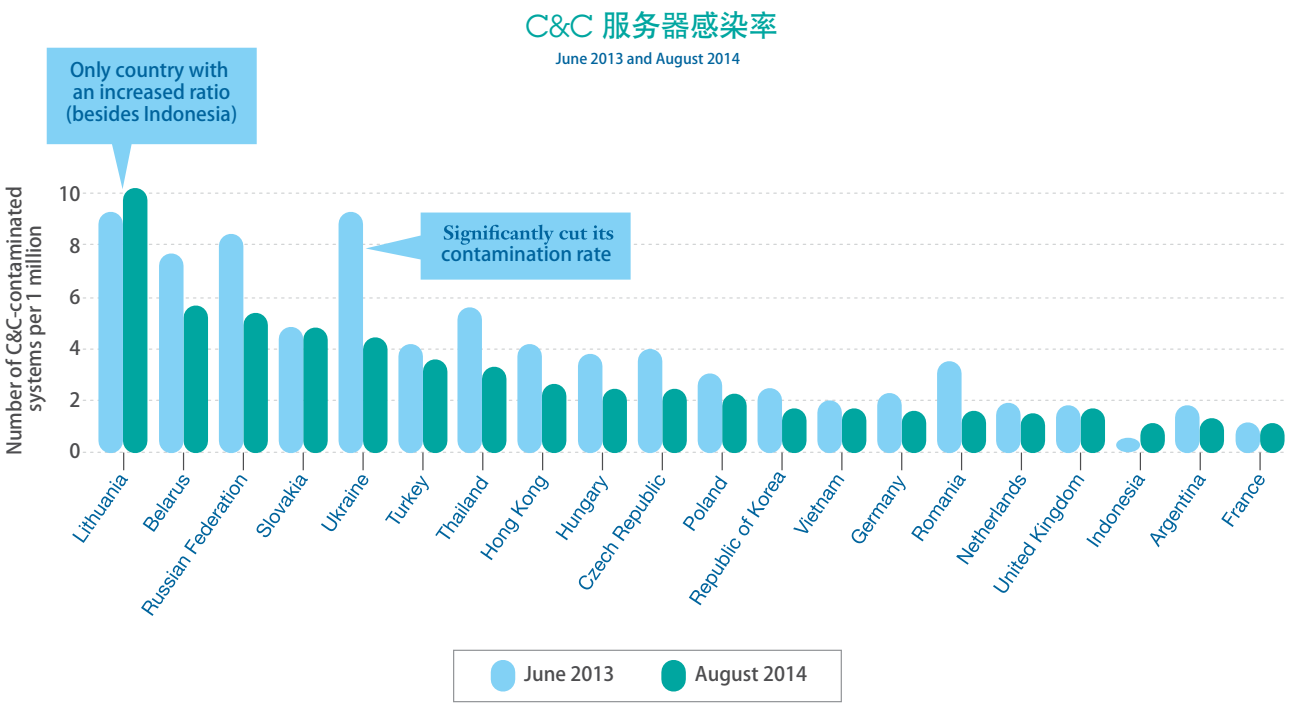


图 5. C&C 服务器感染率，2013 年 6月和 2014 年 8 月

观察总结

有意思是立陶宛占据首位。这与白俄罗斯在垃圾邮件机器人感染率方面领先全球比较相似（欲知有关垃圾邮件机器人感染的更多信息，请参见IBM X-Force威胁情报季度报告 – 2014年第2季度）。

乌克兰东部地区的军事冲突可能是现在其在恶意软件托管方面只占0.7%的原因之一，14个月前来自乌克兰服务器的恶意软件链接比率为1.4%。军事冲突容易中断犯罪企图。而且，随着几乎所有国家的C&C服务器感染总数下降，僵尸网络作业者可能将感染分发到更多的国家，以避免局部地区对这些感染采取的措施。

最后，对于恶意软件托管和C&C服务器受感染国家，东欧国家似乎均排在前列。就像看排在前面的垃圾邮件发送国家一样，看一看这个趋势是否会保持下去以及这一分布是否会改变还是令人感兴趣的（欲知有关垃圾邮件趋势的更多信息，请参见IBM X-Force 2013年中趋势和风险报告）。

关于X-Force

严峻的网络安全威胁无处不在, IBM专家洞见帮助您最大限度降低风险。

IBM X-Force研究与开发团队致力于研究和监测最新网络完全趋势, 包括安全漏洞、漏洞利用 (exploits) 、主动攻击、病毒和其他恶意软件、垃圾邮件、网络钓鱼和恶意Web内容。除了向客户和公众发布有关新出现和高危威胁的信息, IBM X-Force还提供安全内容来帮助保护IBM客户不受这些威胁的侵害。

IBM Security协作

IBM Security代表提供广泛安全能力的多个品牌:

- IBM X-Force研究与开发团队致力于发现、监测和记录广泛的计算机安全威胁、漏洞和最新趋势及攻击者使用的方法。IBM集团的其他事业部使用这些丰富数据来为我们的客户开发保护技术。
- IBM Security Trusteer®20产品族提供了整体式的端点网络犯罪预防平台, 帮助企业防范金融欺诈和数据泄漏。数百家企业和数千万用户依靠来自IBM Security的产品来保护其Web应用、计算机和移动设备不受在线威胁 (如高级恶意软件和网络钓鱼攻击) 的侵害。
- IBM X-Force内容安全团队通过网页抓取、独立发现以及由IBM Managed Security Services (IBM管理安全服务) 提供信息源独立进行Web内容搜寻和分类。
- IBM Managed Security Services负责监测与端点、服务器 (包括Web服务器) 和一般网络基础设施有关的安全漏洞利用。该团队跟踪通过Web以和其他手段 (如电子邮件和即时消息) 来利用安全漏洞的行为。
- IBM Professional Security Services (IBM专业安全服务) 提供企业级安全评估、设计和部署服务来帮助构建有效的信息安全解决方案。
- IBM QRadar® Security Intelligence Platform (IBM QRa-dar®安全信息平台) 提供了包含安全信息与事件管理 (SIEM)、日志管理、配置管理、漏洞评估和异常检测的集成解决方案。它提供统一仪表盘以及对安全和合规风险的实时洞察, 涵盖人、数据、应用程序和基础设施。
- IBM Security AppScan®使企业能够评估Web及移动应用程序的安全性, 加强应用安全项目管理以及通过识别安全漏洞和生成具有完善缓解建议的报告实现法规遵从。IBM Hosted Application Security Management (IBM托管应用安全管理) 服务是基于云的解决方案, 使用AppScan在生产前和生产环境中对Web应用程序进行动态测试。

贡献者

IBM X-Force威胁情报季度报告是一项覆盖全IBM的专业协作。在此我们谨向以下人员为其对本报告的关注和和贡献表示感谢。

贡献者	头衔
Chris Poulin	研究战略家，IBM X-Force
Doug Franklin	研究技术专家，IBM X-Force Advanced Research
Dr. Jens Thamm	数据库经理，IBM X-Force Content Security
Leslie Horacek	经理，IBM X-Force Threat Response
Marc Noske	数据库管理员，IBM X-Force Content Security
Michael Hamelin	首席安全架构师，IBM X-Force
Pamela Cobb	全球市场部经理，IBM X-Force and Threat Portfolio
Ralf Iffert	经理， IBM X-Force Content Security

更多信息

欲知有关IBM X-Force的更多信息，请访问：

ibm.com/security/xforce/

[1] IDC, "Worldwide and Regional Internet of Things 2014–2020 Forecast Update by Technology Split," Doc # 252330, Publish date: November 2014. http://www.idc.com/getdoc.jsp?containerId=252330

[2] Brandon Griggs, "Connected TVs, fridge help launch global cyberattack," CNN, 17 January 2014. http://www.cnn.com/2014/01/17/tech/gaming- gadgets/attack-appliances-fridge

[3] "CES 2014: Toothbrush 'tells you how well you brush',", BBC News, 6 January 2014. http://www.bbc.co.uk/news/technology-25621422

[4] Ellis Hamburger, "Vessyl is the smart cup that knows exactly what you're drinking," The Verge, 12 June 2014. http://www.theverge.com/2014/6/12/5801106/vessyl-smart-cup-that-knows-exactly-what-youre-drinking

[5] Dan Kaplan, "Black Hat: Insulin pumps can be hacked," SC Magazine, 04 August 2011. http://www.scmagazine.com/black-hat-insulin-pumps- can-be-hacked/article/209106/

[6] Steve Henn, "With Smarter Cars, The Doors Are Open To Hacking Dangers," NPR, 30 July 2013. http://www.npr.org/blogs/ alltechconsidered/2013/07/30/206800198/Smarter-Cars-Open-New- Doors-To-Smarter-Thieves

[7] "Online Energy Monitoring," Consumers Energy, Accessed 08 October 2014.http://www.consumersenergy.com/content.aspx?id=1696

[8] Robert Vamosi, "Hard-coded Credentials Still Haunt Many Legacy IoT Products," Forbes, 13 August 2014. http://www.forbes.com/sites/ robertvamosi/2014/08/13/hard-coded-credentials-still-haunt-many- legacy-iot-products/

[9] "Experimental Security Analysis of a Modern Automobile," 2010 IEEE Symposium on Security and Privacy. http://www.autosec.org/pubs/cars-oakland2010.pdf

[10] Dan Goodin, "Intruders hack industrial heating system using backdoor posted," Ars Technica, 13 December 2012. http://arstechnica.com/ security/2012/12/intruders-hack-industrial-control-system-using- backdoor-exploit/

[11] Dan Goodin, "Crypto weakness in smart LED lightbulbs exposes Wi-Fi passwords," Ars Technica, 7 July 2014. http://arstechnica.com/ security/2014/07/crypto-weakness-in-smart-led-lightbulbs-exposes- wi-fi-passwords/

[12] Danny Yadron, "Russian Hackers Steal 1.2 Billion Usernames and Passwords, Security Firm Says," Wall Street Journal, 05 August 2014. http://blogs.wsj.com/digits/2014/08/05/security-firm-russian-hackers- amassed-1-2-billion-web-credentials/

[13] "'Password' unseated by '123456' on SplashData's annual 'Worst Passwords' list," SplashData, Accessed 21 October 2014. http://splashdata.com/press/ worstpasswords2013.htm

[14] John Lucassen, "Are Vendors Doing What Is Needed to Mitigate Security Vulnerabilities?" IBM Security Intelligence Blog, 30 June 2014. http://xforce.iss.net/xforce/xfdb/92322

[15] Seth Hanford, "Common Vulnerability Scoring System, V3 Development Update," FIRST, June 2014. http://xforce.iss.net/xforce/xfdb/96153

[16] OWASP Internet of Things Top 10 Project. https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

[17] IBM Institute of Business Value, "Transforming the automotive industry: A globally integrated enterprise point of view," 05 September 2014. http:// public.dhe.ibm.com/common/ssi/ecm/en/gbe03619usen/ GBE03619USEN.PDF

[18] "Vulnerability Disclosure Policy," CERT. Accessed 08 October 2014.http://www.cert.org/vulnerability-analysis/vul-disclosure.cfm

[19] IBM, "IBM Internet Security Systems X-Force Research and Development Team Vulnerability Guidelines," December 2008. http://www-935.ibm. com/services/us/iss/xforce/vulnerability-guidelines.pdf

[20] Trusteer, Ltd. was acquired by IBM in September of 2013.

国际商业机器中国有限公司
北京市朝阳区北四环中路27号
盘古大观写字楼
邮编: 100101

在中国印刷

2014年12月

WGL03062-USEN-00