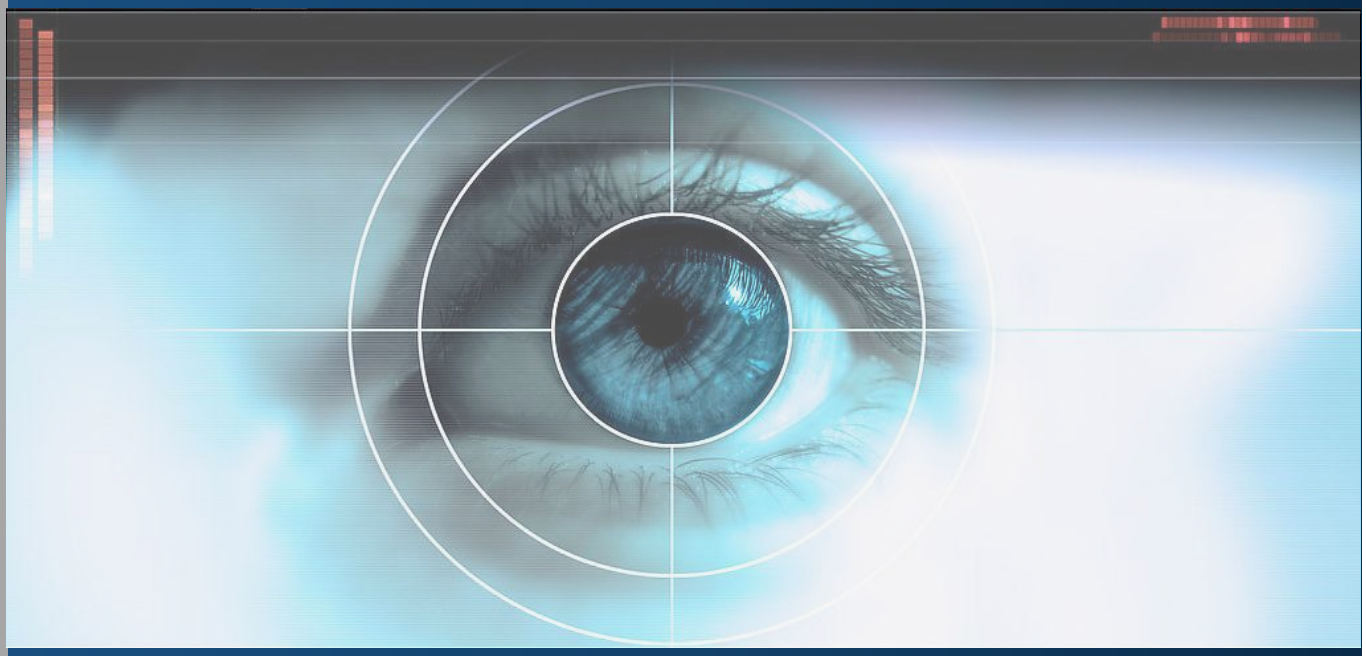
ANTIY 安天



回眸 2014，网络安全那一瞬

——2014 年网络安全年度简报

安天实验室 安全研究与应急处理中心

目 录

1 引子

2014 年，对于网络安全来说，充满了不宁静与不寻常。这让我们觉得，每年那些长篇累牍的从恶意代码后台系统中导出的统计数字，无以表征这个既“波澜壮阔”又“波谲云诡”的年代。因此，我们决定用若干幼稚的文字和图表，对这一年做一个简要的回望。

早在一年前，即 2014 年新年的时候，安天依然像每年一样，更新安全威胁主题的通缉令扑克，来作为新年礼物。我们把 APT(Advanced Persistent Threat，高级持续性威胁)选为大王，以认定这是最严重的安全威胁；而把 Malware/Other 作为小王，以作为安全威胁趋势演进的预测，这是一个依托恶意代码命名法的自造词，我们把它的中文名字称为——“威胁泛化”。

2 APT

“APT 热度是否在下降”？2014 年，这个问题多次在我们的技术演讲后，被听众或媒体问起，对此，我们给出的回答是，当媒体对一个威胁产生审美疲劳时，往往是这种威胁已经走入常态化，其不再只是突击研究，而是开始逼近更多人的身边。

而如果从 APT 这个词从 2005~2006 年间，在美国空军第八联队的会议室中被创造出来算起，其已经具有 8 年的历史，其本身已经被太多地解读和咀嚼。而其热度乍起，是在 2011~2012 年，一些新的产品解决方案逐步成熟，并被产业和舆论关注的结果。

从这个意义上说，对于在 2005~2006 年，还依然更多关注木马的快速数量膨胀影响的我们来说，已经“迟到了”！

2014 年，谈及 APT，无疑公众更关注电影《The Interview》所导致的发行商索尼影音公司遭遇的入侵和破坏事件。但从另一个角度来看，当一个攻击以敲诈式的警告于前，而以破坏硬盘数据为结尾的时候，它还是一种 APT 么？也许与 Michael 在《Why Stuxnet Isn't APT》中质疑 Stuxnet 是 APT 还是 Cyberwar 一样，索尼事件也许同样是一种作战行动，只是其技术手法显得没有那样高明而已。

APT 事件依然更多地为“注意力”所牵引。在整个 2014 年曝光的 APT 攻击事件共有 33 起，其中 Regin 和 Epic Turla 为攻击国家和组织数量最多的事件。Regin 是一组先进隐形的恶意程序，具有高明的隐藏手段，并且使用了 P2P 技术进行发送指令和窃取信息。从其身上，我们才真正能看到与 APT 一词所匹配的艺术式的攻击手段和制式化的装备体系。

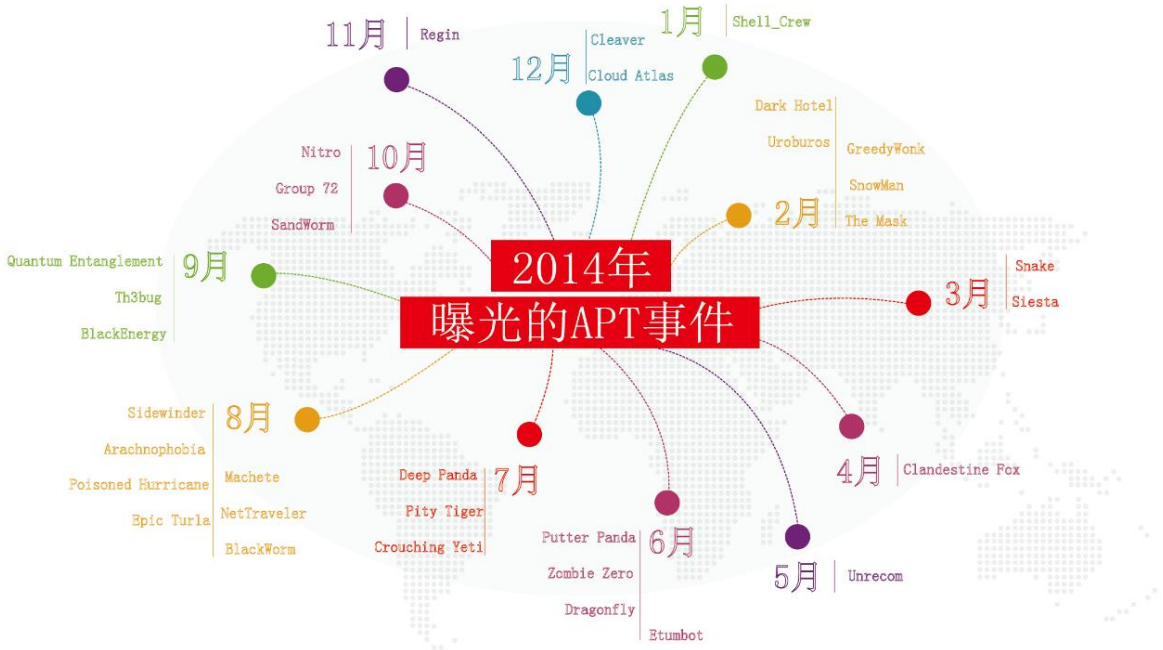


图 1 2014 年曝光的 APT 事件

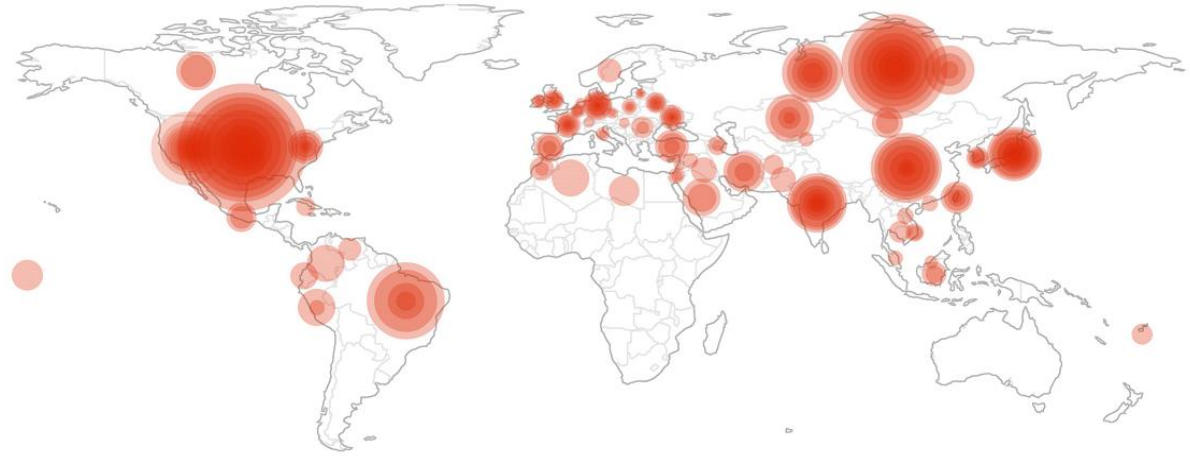


图 2 2014 年曝光的 APT 事件中被攻击国家

2014 年被曝光的 APT 事件攻击了近百个国家，其中遭受攻击最多的也正是美国、俄罗斯、中国、日本等全球国家。主要被攻击的行业为能源、金融、医疗保健、媒体和电信、公共管理、安全与防务、运输和交通等行业。

3 严重漏洞

2014 年 4 月 7 日，发生了被称为 3 年来最严重的漏洞 Heartbleed（心脏出血）漏洞，这个漏洞存在于开源密码技术库 OpenSSL 中，该漏洞会导致内存越界，攻击者可以远程读取存在漏洞版本的 OpenSSL 服务器内存中 64K 的数据，从而可以被用于获取内存中的用户名、密码、个人相关信息以及服务器证书、私钥等敏感信息。由于 OpenSSL 使用非常广泛，因此这个漏洞影响到了包括 Google、Facebook、Yahoo 以及国内 BAT 在内的大型互联网厂商，以及大大小小的网银、电商、网络支付、电子邮件等各种网络服务厂商和机构。

漏洞存在于 OpenSSL 中已有两年之久，后被谷歌研究员尼尔·梅塔（Neel Mehta）与网络安全公司 Codenomicon 的研究员发现，他们通知了 OpenSSL 组织进行漏洞修补工作。漏洞公告发布时已发布了修补漏洞的新版本 OpenSSL 1.0.1g，同时 Google 也比业界更早地修补了漏洞。而漏洞公布后，网络攻击者们也开始疯狂地获取数据，有人开玩笑的说，为了存放通过 Heartbleed 获取的数据，导致了硬盘价格的上涨。虽然言过其实，但其利用价值可见一斑。而当我们回看类似事件时，Codenomicon 等一些新锐公司为了提高知名度不负责任的发布 POC，也是威胁“泛化”的重要原因。

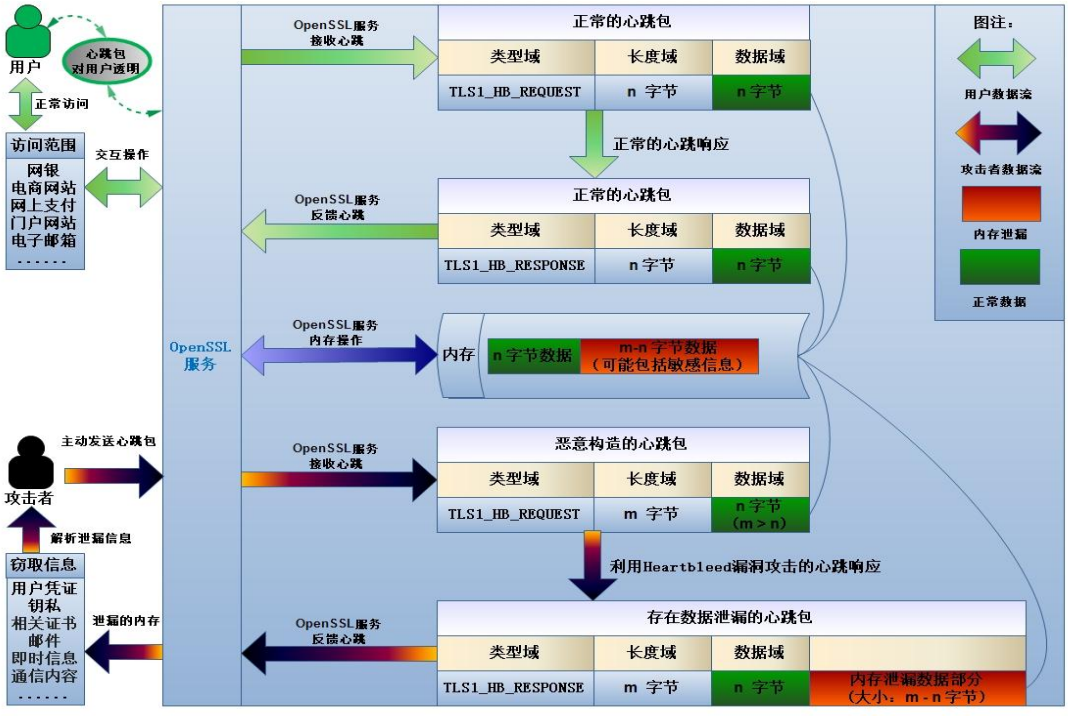


图 3 Heartbleed 原理图

注：图 3 引自安天《Heartbleed 漏洞（CVE-2014-0160）FAQ》（http://www.antiy.com/response/heartbleed_faq.html）

而到了 9 月，则再次曝光了比“心脏出血”更严重的漏洞——“Bash Shellshock”（破壳），由于 GNU Bash 更广泛的存在，导致其所威胁到的不仅仅是服务器系统，也包括了网络设备、网络交换设备、防火墙等网络安全设备，也包括摄像头、IP 电话等很多采用 Linux 剪裁定制的系统。经过研究发现，这个漏洞已经存在了近 20 年。而另一个致命的问题是，由于 GNU Bash 的分布蔓延极广，几乎是无法完全定位修复的；而且由于 Bash 灵活的语法，导致解析程序极为复杂，因此在几次修补方法公布后，都随即被发现了新的问题，从而使“破壳”演化了一系列的漏洞。

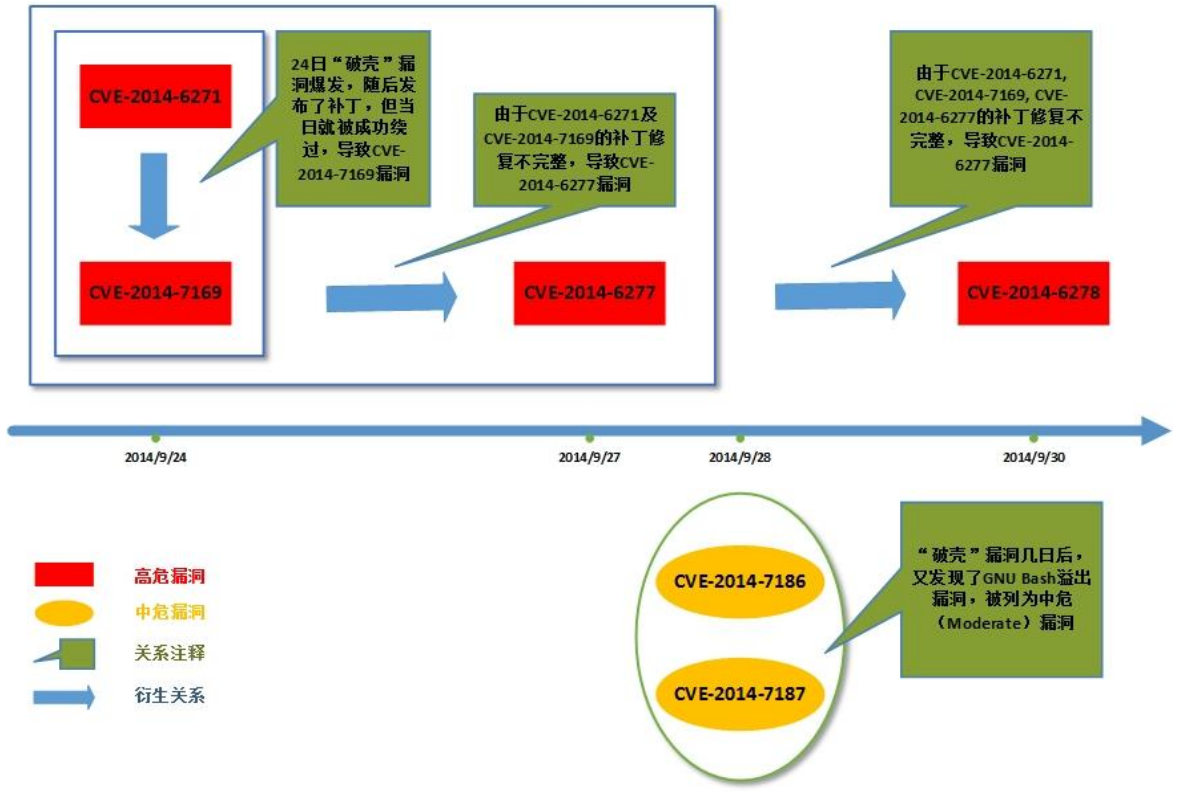


图 4 “破壳”漏洞的披露与修补迭代

注：图 4 引自安天《"破壳"漏洞的关联威胁进化与类 UNIX 系统的恶意代码现状——“破壳”相关分析之三》（http://www.antiy.com/response/The_Association_Threat_Evolution_of_Bash_and_the_Current_Status_of_Malware_in_UNIX-like_Systems.html）

再之后，一场持续的 DDoS 攻击，严重影响到了国内 DNS 体系的运行，而大量发起攻击的节点则是摄像头等在网智能设备，而经跟踪分析相关僵尸网络，其正是利用了“破壳”漏洞扩展获取了大量的节点。

其实在一些国产操作系统上，我们也同样发现了“破壳”漏洞的存在，理顺国产系统的借鉴、继承关系，及时联动地漏洞修补，对于依托开源体系发展的国产操作系统领域来说，依托开源软件的伪闭源系统，其实比开源软件本身有着更大的漏洞威胁。

此外，HTTPS 作为安全认证和加密通讯的重要基础协议，在这一年被反复提起，微软 Server 的 SSL 实现也被发现存在问题，而多家网银亦都被暴露出不正确的代码实现。

4 安全威胁的泛化与分布

2014 年除我们熟悉的 Windows、Linux 和其他类 Unix 系统、iOS、Android 等操作系统及其应用软件漏洞外，随着智能家居、穿戴硬件以及信息化在社会生活中的无所不在，威胁也在跟随演进。我们做了一个图表来尝试说明威胁的分布演进。

图 5 2014 年网络安全威胁泛化与分布

5 数据泄漏

2012 年的系列“拖库门”导致的数据泄露事件曾引起很大的影响，而 2014 年的数据泄露问题依然严重，这些泄露的数据有的依然来自拖库，但有的则来自撞库攻击。而其中影响颇大的“12306 撞库攻击事件”，则让人们看到传播一些通过撞库形成的少量数据集合，用以声称后台数据泄露，就会造成一定社会恐慌。

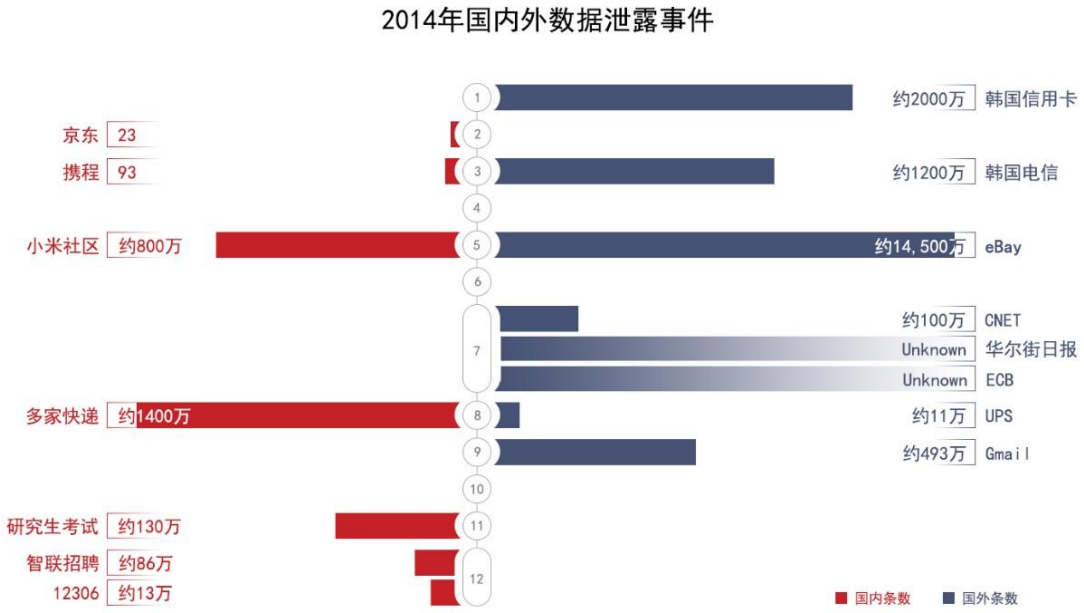


图 6 2014 年国内外曝光的重大数据泄露事件

我们此前对“12306 撞库事件”中的泄漏数据做了一点统计，这说明，未来网站服务者依然需要引导用户去实现更强壮的密码策略，特别是为重要网站使用单独的口令。

	口令	用户数量	比例
1	123456	392	0.30%
2	a123456	281	0.21%
3	123456a	165	0.13%
4	5201314	161	0.12%
5	111111	157	0.12%

表 1 12306 泄露数据中的 TOP5 口令

	数量（未消重）	比例	数量（消重后）	比例
口令数量	131653	100.00%	117808	89.48%

口令中含有特殊字符	177	0.13%	154	0.12%
纯数字口令的用户	35572	27.02%	30456	23.13%
纯字母口令的用户	7161	5.44%	6004	4.56%
纯小写字母口令的用户	6947	5.28%	5797	4.40%
纯大写字母口令的用户	62	0.05%	61	0.05%
大写字母+数字	395	0.30%	383	0.29%
小写字母+数字	87664	66.59%	80133	60.87%
大小写字母混合+数字	237	0.18%	228	0.17%
密码中含有生日（8 位，例如 19810101）	3400	2.58%	1725	1.31%
密码与生日相同（8 位，例如 19810101）	2326	1.77%	3322	2.52%
密码中含有生日-但非本人的生日（8 位，例如 19810101）	11368	8.63%	10269	7.80%
密码中不包含生日的	114559	87.02%	102889	78.15%
用户名与口令同（同一条数据）	1733	1.32%	1712	1.30%
用户名与口令同（不是同一条数据）	1769	1.34%	1746	1.33%
口令部分包含用户名（同一条数据）	832	0.63%	820	0.62%

表 2 12306 泄露数据中的密码使用习惯统计

6 PC 平台恶意代码

我们曾在《木马雪崩到 APT 的关联与必然》中就 2006~2012 年恶意代码的快速爆炸式增长进行了分析，而这种趋势目前又有了很大变化。从入库黑样本数量来看，2014 年，我们的样本库新增了 3000 万个 Hash，但增速已经大大放缓。

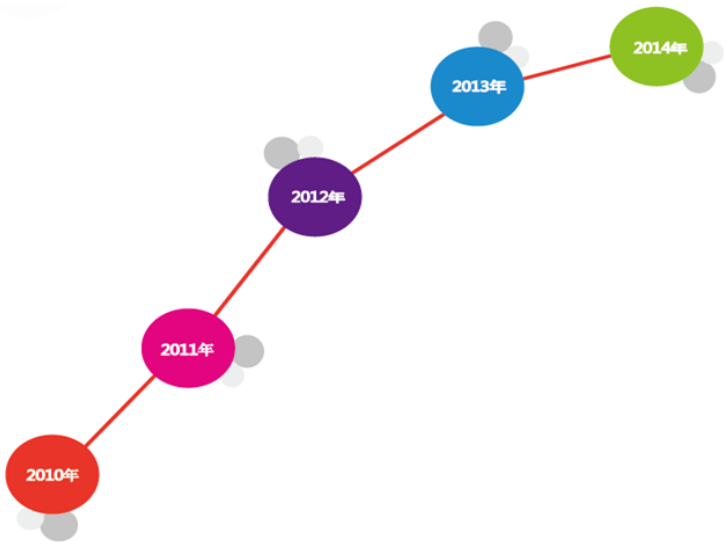


图 7 近五年恶意代码数量增长趋势

2014 年，PC 平台的恶意代码家族新增样本数量排行榜，排在首位的则是 2014 年 2 月产生的名为 Trojan/Win32.AntiFW 的恶意代码家族，该恶意代码家族以获取经济利益为目标，具有潜在的威胁，包括安装广告软件、劫持浏览器、尝试修改浏览器首页、自定义搜索设置等行为。

在 TOP10 排行榜中，有 5 款类似的广告软件家族，其目标相同，大都是以获取经济利益为目的，分别为 DomaIQ、Lollipop、Morstar、AdLoad、MultiPlug。从首次出现的时间上来描述，可以发现除 GrayWare[AdWare]/Win32.AdLoad 外（2011 年出现的广告件家族），大部分都为近期新产生的广告软件家族。

在 2014 年恶意代码数量排行榜中，并未出现新的感染式恶意代码家族，占据感染式病毒排行榜前列的仍然是 Sality 和 Virut 两个老样本，同时，Nimnul 家族依然在榜。在 TOP10 排行榜中，排在最后的为组建僵尸网络的 Zbot 家族，这个家族在 2014 年依然挥之不去，并通过邮件等手段传播。

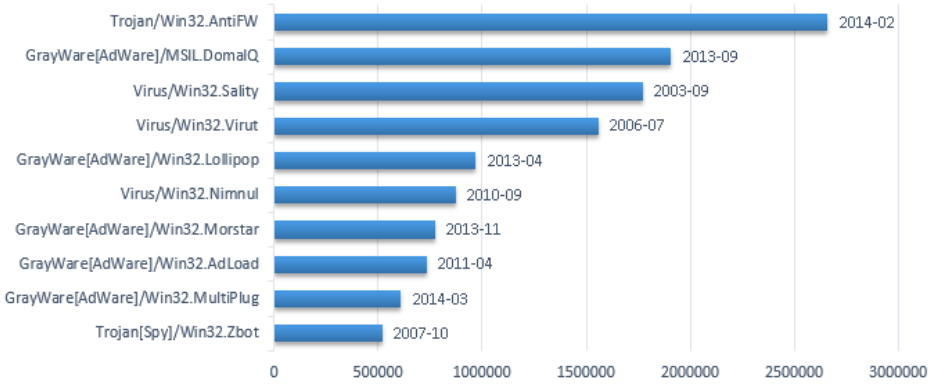


图 8 2014 年 PC 平台恶意代码数量排行榜

2014 年 PC 平台恶意代码行为分类排行中，以获取利益为目的的广告行为再次排在第一位，下载行为因其隐蔽性、实用性强的特点数量依然较多，具有远程控制行为的后门类恶意代码排在第三位。

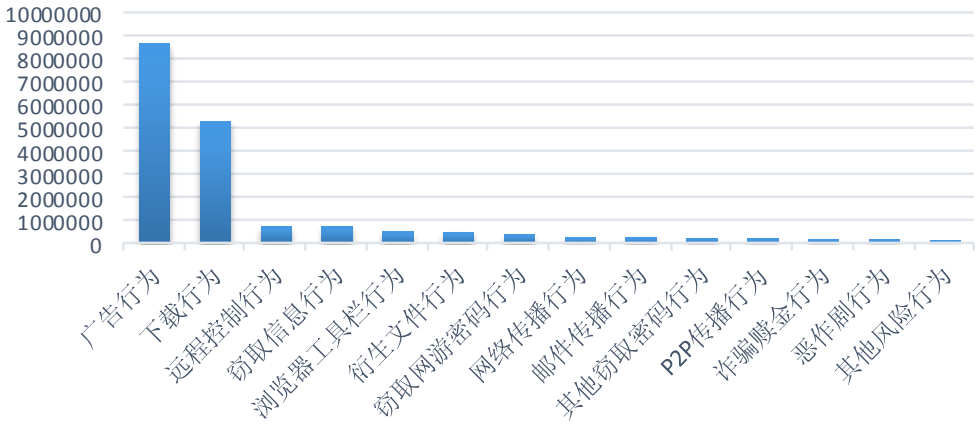


图 9 2014 年 PC 平台恶意代码行为分类排行榜

7 移动平台恶意代码统计

2014 年移动平台的恶意代码数量增长趋势较 2013 年同样略有放缓，全年入库样本数量已经超过 80 万。

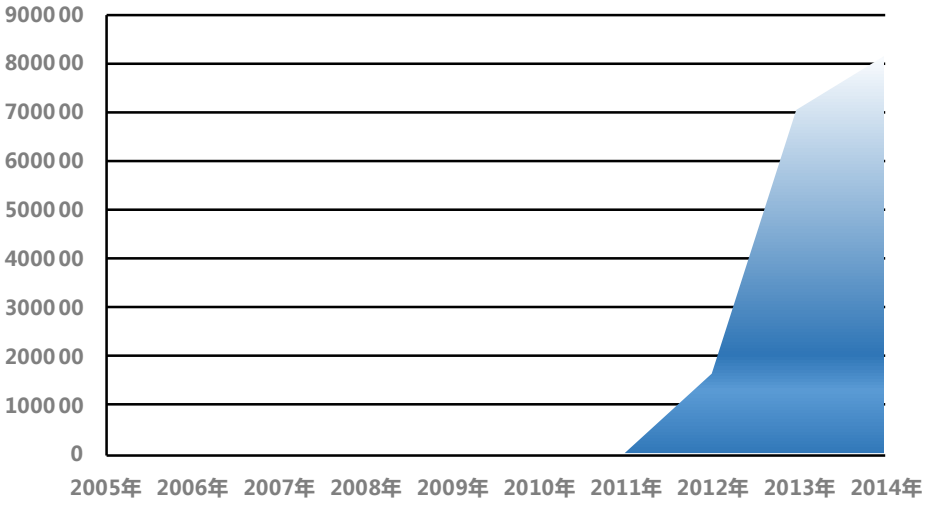


图 10 2005 年-2014 年移动平台恶意程序走势

移动平台恶意程序按行为分为 8 类：恶意扣费、资费消耗、系统破坏、隐私窃取、流氓行为、远程控制、诱骗欺诈、恶意传播。

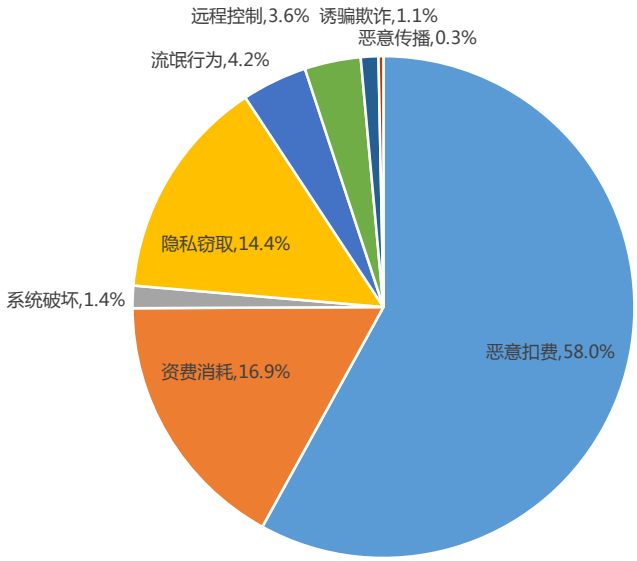


图 11 2014 年移动平台恶意程序数量按行为属性统计

2014 年移动平台恶意程序传播事件次数月度统计，3 月份传播次数最高，接近一千二百万次，12 月份传播最低。传播次数中可以看出，上半年和下半年都呈现出了两次下降趋势。

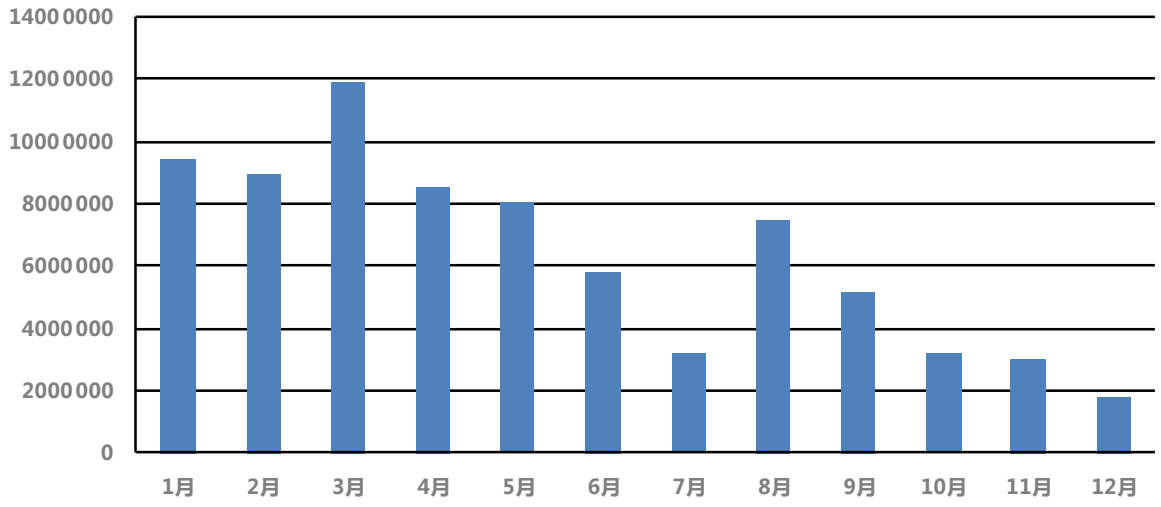


图 12 2014 年移动平台恶意程序传播事件次数月度统计

2014 年移动平台恶意程序传播源域名和 IP 数量月度统计，可以看出使用域名访问是恶意程序传播较多的选择。

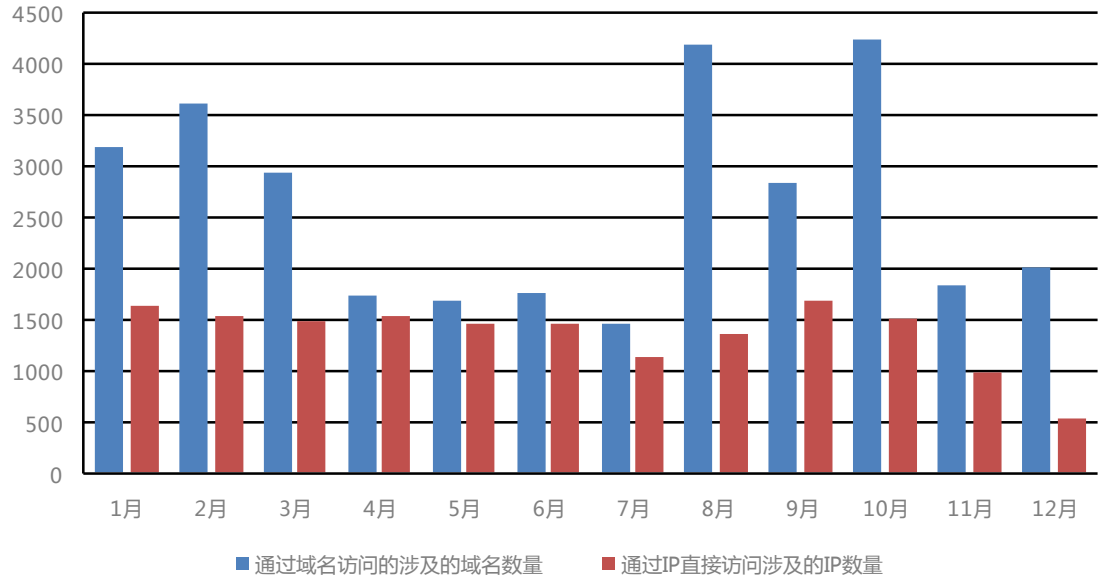


图 13 2014 年移动平台恶意程序传播源域名和 IP 数量月度统计

8 泛化年代的思考

2014 年，威胁泛化的年代，是一个打破幻像的时代。例如之前所谓的开源安全神话，当少数开源安全论者还在坚持着“开源是全世界一起做一个系统，闭源是少数人做一个系统”的时候，社区因安全能力不平衡所带来薄弱环节的影响正在凸显。Heartbleed 就在最常见的 OpenSSL 中展示了“灯下黑”的结果，并提醒业界这正是达成安全所需要聚合的安全专业性、研究能力以及配套的安全成本。而另一方面，心脏出血后这场针对开源系统安全普查的业内联合行动，或许可以被看成一场灾难的“进步补偿（恩格斯语）”。这种活动让开源体系真的从全域威胁的角度获得了审视。而 Wirelurker（破界），同样让 iOS 的安全神话破灭。

2014 年，关键漏洞再度展示了“一览众山小”的巨大能量，其让原有的那些漏洞数量的比对和哪种系统更安全的空泛讨论完全失去了意义，关键漏洞给攻防双方都带来了很大的不确定性和偶然性，信息攻防强弱之能力可能在瞬间被一个关键漏洞拉平。

泛化的年代是一个盲目的时代，当新威胁被反复强化，我们很容易被吸引而目光游移，我们很容易完全去关注新威胁，而不去分析我们的基础和家底，而后者同样重要。比如在 Heartbleed 中，同样令人值得思考的问题是研究者们同时注意到，国内网站的 HTTPS 使用比率很底，大量网站依然采用 HTTP，包括有著名的网站（包括手机端）居然采用明文登陆协议，安全措施只是口令计算了一个 Hash 而已。这实际上是中国和发达国家在安全基础意识和能力上的代差。

而今年同样流行着对“老三样”——即“防火墙”、“反病毒”、“打补丁”的口诛笔伐。这种声讨被用于支撑去寻觅一个新的安全模型或思维。但实际上，在中国更多政企用户中更真实的情况是大量防火墙被采购后，被束之高阁，从未被安装和加电；内网反病毒产品的病毒库几月到半年才升级一次，而“打补丁”更被视为有可能影响业务稳定性的危险举动。我们现有的安全问题更多的是来自“老三样”不管用？还是没有真正重视和有效使用？

从互联网安全服务规范到 IT 治理能力，我们在安全上有很多课要补，我们并非已经建立了充分夯实的体系，可以把目光充分转移去审视新威胁，而是需要同时面对新旧两种挑战。而如果我们漠视这些现状，就会催生不切实际的误判，特别是开始膜拜和憧憬所谓一劳永逸改变安全现状的“永动机”，而忘记了安全的本质就是永无休止的对抗与改进。

泛化的年代亦可能是一个麻木的时代，比“心脏出血”更为严重的“破壳”漏洞却难以得到更多来自国内媒体的关注，原因竟然是很多人认为 “心脏出血没有造成那么大的影响”。当一些主流网站（包括电商）的内存数据被以 T 为计的获取时，我们实在无法想象，还有什么是更大的影响。只有大面积断网、大

量的后台数据被直接公开才算重大影响吗？这是一种何其落后的安全判断标准，这种思维定式足以使人在即将喷发的火山口上载歌载舞。

威胁泛化出现的原因，首先是信息化大发展注定使其无所不在，而很多的陷阱、隐患和错误的思维在不断的被继承，这是威胁泛化注定的土壤；其次是攻击能力的普及化，正如 Bruce Schneier 在《The State of Incident Response》所说“正在发生而且真正重要的趋势是：越来越多战争中的战术行为被应用于更广泛的网络空间环境中。”，这为加速威胁泛化提供了工具弹药；而地下黑产的蓬勃发展，追名逐利日益无底线，也成为威胁泛化的持续动力。

泛化的年代，让很多人重新萌生了计划经济式的预设情节，对安全的恐慌，导致很多关于“不设计好安全就不要发展的观点”重新浮出水面。这些观点忽略了需求的刚性，认为通过沙盘推演和标准设定能解决很多问题。

在威胁泛化的年代，更多人会想到 K.K 的《失控》，而一位我十分尊重的老师告诉我，在他的案头有两本书，一本是《失控》，而另一本是来自比尔.盖茨的《未来之路》，他说“从目前来看，对于一个未来的高技术的世界，前者带给人们的焦虑和恐慌远胜于后者曾带给人们的憧憬，但想一想，蒸汽机、电器机、原子能、基因技术……哪一项巨大的技术进步不曾带给人类巨大的、仿佛毗邻悬崖边缘的焦灼？但这一切尽管亦曾被用于破坏、犯罪和战争，但最终我们的世界始终是变得更文明、发达和美好。”

安全的存在意义从来都是用于保障应用价值，而不是用来限制应用价值，更不是用来捆住发展的手脚。而今天，尽管我们面对种种安全危机，以及伴生的对未来的种种焦虑，但我们一直坚信发展、进步才是最大的安全。

安全工作者要做实干者，而非预言家，也许这一选择更适用于“沧海横流”的时代。

附录一：关于安天

安天是专业的下一代安全检测引擎研发企业，安天的检测引擎为网络安全产品和移动设备提供病毒和各种恶意代码的检测能力，并被超过十家以上的著名安全厂商所采用，全球有数万台防火墙和数千万部手机的安全软件内置有安天的引擎。安天获得了 2013 年度 AV-TEST 年度移动设备最佳保护奖。依托引擎、沙箱和后台体系的能力，安天进一步为行业企业提供有自身特色的基于流量的反 APT 解决方案。

关于反病毒引擎更多信息请访问： http://www.antiy.com（中文）

http://www.antiy.net（英文）

关于安天反 APT 相关产品更多信息请访问： http://www.antiy.cn

附录二：文档更新日志

更新日期	更新版本	更新内容
2014-12-25 13:58	V1.0	撰写
2015-01-15 16:53	V1.1	修改数据、图表等
2015-01-18 14:11	V1.2	修改文字
2015-01-29 10:21	V1.3	较对