信息安全A-Z

文 / 肖新光

2012年的信息安全是散乱的——话题众多却没有绝对的焦点，热门企业与人物纷纷登场却没有绝对的主角；2012年的信息安全是焦灼的——风声鹤唳、草木皆兵，一切环节皆发生威胁，一切环节又皆可构筑防御。这些都给这篇对2012年信息安全进行总结的命题作文带来了难度。当话题无法被收拢时，我们唯有将其陈列；当它们主次难分时，我们只能按字母顺序排列。于是就有了这篇《信息安全A-Z》。

A APT（Advanced Persistent Threat，**高级可持续威胁**）：这并不是一个全新的词汇，但毫无争议地成了我们的开篇词。这种带有政府和政经集团背景的、不惜代价的、集威胁方法与经验之大成的威胁形式，有可能带来整个安全产业新一轮的技术竞赛和产品更新。

B Big Data（**大数据**）：这在2012年是一个酷热的主题，大数据时代的到来是网络信息社会发展的必然。站在信息安全的角度，高增长的带宽和信息的膨胀，无疑为攻击者提供了隐匿的空间，从而增加了守护者的负担；但从好的一面来看，存储和计算能力的增长也带来了大数据长期缓存和挖掘分析的可能性，从而也为安全分析工作带来了新的方法和机遇。

C Cloud Security（**云安全**）：云的安全随着云应用的落地而被重视起来。今年，CDN、SDN的倡导者们都在各种安全论坛上宣称着自身架构的优势，云的安全性应该由云服务提供者自己解决还是应该交给安全产业界来解决，也各有不同观点。

D Doubt（**怀疑**）：这不是一个技术术语，但怀疑和不信任的氛围弥漫在2012年的整个世界。美国众议院《对中国电信公司华为与中兴引发的美国国家安全问题的调查报告》就是其典型的代表，报告行文的背后，贸易保护主义味道浓郁。从多次对日本汽车的打压，到对三星的专利诉讼，在美国，类似的保护主义并不罕见。然而，与这些不同的是，国家安全命题显然是绕开WTO规则的最佳选择。但以国家安全的名义推行贸易保护主义，对于两个自身都有很大市场空间的大国来说，留下的将不只是产业的裂痕。

E Embedded Device（**嵌入式设备**）：嵌入式设备的安全一直是这几年来被关注的焦点。2012年，一款集成了Wi-Fi、3G、以太网等功能的渗透测试用插线板被曝光，这让嵌入式系统的攻击价值凸显出来。更值得关注的是，这款设备是DARPA（美国国防部高级研究计划局）公开资助项目的成果。

集成了Wi-Fi、3G、以太网等功能的渗透测试用插线板（图片来源：http://securityaffairs.co）

F Flame（**火焰病毒**）：这无疑是今年最令整个安全业界关注的恶意代码。从系列域名的

分析到其中一些文件组件找到线索，说明这个病毒家族大概从2007年底或2008年初就开始活动。这种产业界整体的后知后觉更见证了APT攻击的巨大能量。

G Government Attack（政府攻击）：美国和以色列是否与Stuxnet病毒有所关连，此前只是从“谁是受益者”的角度，把两国政府作为了怀疑对象。而在2012年美国大选期间，有美国政府背景的“深喉”出现，声称此事有美以两国联合的背景。有分析人士认为，这种“泄密”是为了在选战前强化奥巴马政府的行动力和果敢倾向，就像海豹小组成员根据击毙本·拉登所写的No Easy Day（《艰难一日》）一书的效果一样。

H High Level Operational Concept（高等级网络作战原则）：美国国防部开始正式确立相关Cyber War（网络空间战）的作战规则，在英国政府的有关公开文献中也能看到这个语汇，印度也有所参与。

I IPv6：中国国家发改委2012年面向IPv6的快速发展和应用，对下一代高带宽、高性能的八大类网络安全设备进行立项支持。与既往专项不同的是，本次组织了国内权威测试机构对申报产品直接进行严格测试，以测试结果决定是否进行支持，完整测试结果计划上网公开，通过测试产品进入相应产品名录，并一次性拿到多个资质，为国内具有技术能力的安全企业和产品降低了行政准入门槛。

J Jailbreak（越狱）：越狱问题在封闭的苹果产业链上打开了一个缺口，带来了进一步的乐趣与活力，也带来了连锁的安全问题。2012年，民间团队iPhone Dev Team、Chronic Dev Team以及pod2g合作发布了Absinthe工具，并进行多次版本更新，先后对iPhone 4S、iPad 2和The New iPad实现了越狱破解。

K Kelihos（一种僵尸网络）：2012年1月，微软宣布查出了Kelihos僵尸网络的作者是俄罗斯圣彼得堡的一位计算机工程师。这个僵尸网络此前被微软通过技术和法律手段清除了。

L Legislation（立法）：信息安全立法滞后问题在今年的一些产业纠纷中暴露出来，互联网客户端对隐私采集的边界到底是什么、robots协议是否具有约束力等，都是今后司法界要面对的课题。

M Mobile Security（移动安全）：安全保护在2012年开始逐渐成为移动设备的标配。而且不仅限于个人安全，BYOD概念的提出让手机安全环节与传统企业IT治理环节成为一个整体；Android恶意代码继续飞速增长，中国和俄罗斯成为这些恶意代码的主要源产地。

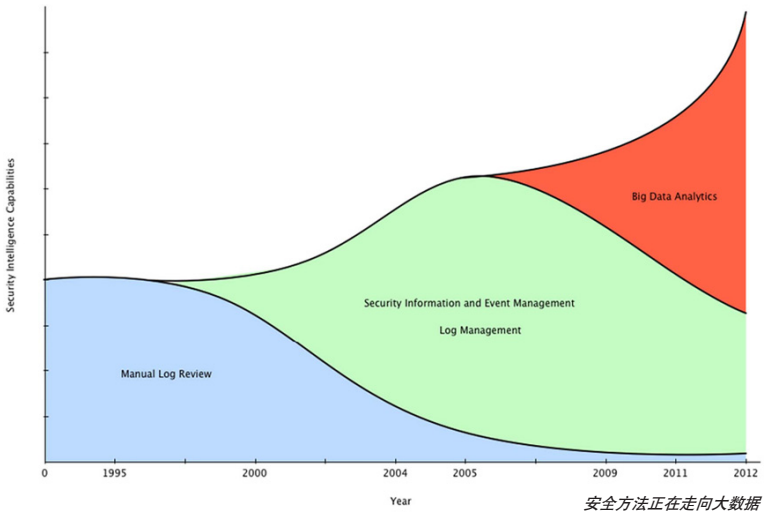
N NG-FW（Next Generation Firewall，下一代防火墙）：这一概念在其被提出了多年之后，终于结出了产业果实，其概念创造者Palo Alto Networks于2012年7月20日在纽约上市，IPO表现强劲，上市当天市值为26亿美元，截至2012年11月14日市值为36.4亿美元。

O OAuth 2.0（一种开放式认证协议的2.0版本）：作为一种新兴的网络认证方法，目前众说纷纭，褒贬不一。尽管微软和Google都对OAuth提供了API支持，但其作者Eran Hammer却于2012年6月辞职，并且声称“OAuth2.0是一个坏的协议”。

P Privacy（隐私）：互联网寡头的隐私侵害威胁2012年被广泛关注。Google、苹果、Facebook都遭到反复质疑，而微软和Google之间关于浏览器隐私浏览模式和P3P协议之争，正体现着传统收费厂商和互联网免费厂商之间在理念和模式上的巨大博弈。

Q QR Code Security（扫描码安全）：很早以前，就有人预言过二维码的安全问题，甚至多家企业都预先申请了检测这类攻击的专利。2012年下半年，用户才真正遭遇到这类攻击。伴随着手机平台一些浏览器漏洞和系统残留内部指令被发现，利用二维码进行的攻击可能会成为更加严重的问题。

R Root Cause Explorer（溯源）：在APT攻击逐渐被认为难以避免和防范的背景下，有



安全方法正在走向大数据

效的追踪溯源方法成为2012年研究界和产业界的重点话题。

S SHA-3（美国标准散列算法）：美国下一代标准散列算法的遴选历经两年终于产生结果，Keccak在2012年10月3日笑到最后，被NIST（美国国家标准与技术研究院）选中，这是一个基于海绵结构（sponge construction）的海绵函数（sponge function）的算法，证实了此前关于M-D结构将被束之高阁的预言。

T Timing Related Threats（时间相关的威胁）：2012年，出现了多起因为时间同步问题而导致的重大金融事故。另一方面，Antiy Labs的两位博士也在2012年8月的XCon会议上以“攻击时间”为主题，演示了对长波授时信号的干扰和仿冒。

U UUID（Universally Unique Identifier，通用唯一识别码）：著名黑客组织Anonymous宣布在AntiSec行动中入侵了FBI的电脑，获取到并公布了一批苹果用户移动设备的UDID及其他信息，Anonymous据此指责FBI侵犯公民隐私，而FBI则予以否认。之后美国佛罗里达州一家名为BlueToad的出版公司声称这些数据来自他们的数据库。由于各方均未有效自圆其说，成为一起隐私“罗生门”事件。

V Virtual Computing Security（虚拟计算安全）：云的架构和安全性很大程度建立在虚拟计算基础上。2012年，多个能对虚拟化系统实现穿透的漏洞和攻击模式被发现。另一方面，对采用虚拟机进行恶意代码自动化分析的研究者来说，如何有效对抗恶意代码反虚拟机技术，也成为一个必须解决的问题。

W Windows 8：Windows 8在2012年10月26日正式发布，除了全新操作体验之外，安全环节也得到进一步增强，DEP、ASLR、UAC等机制均得到了强化，沙盒、预装杀毒软件、UEFI安全机制也开始加入。

X Xtreme RAT（一种后门工具）：这是一款老资格的后门工具，之所以能上榜在于，它不仅是最早一批号称支持Windows 8的后门，而且出现在入侵以色列的场景中。

Y Yahoo! Password Leakage（雅虎密码泄露）：2012年7月11日，雅虎近45万账户密码被盗，攻击者据称采用了老套的union-based SQL injection的攻击手法，这也是2011-2012年一系列拖库事件的余音。放在波谲云诡的2012年信息安全乱象中，这或许都不能算一件大事，反而是为Yahoo!这个老牌互联网厂商的江河日下增加了注脚。

Z Zeroaccess（一种僵尸网络）：这是一款采用rootkit技术的botnet，在2012年10月被业内关注。我们选择Zeroaccess作为Z的关键词：一方面是提醒各种安全威胁合流的趋势；另一方面，对每年选择Zero Day作为Z的关键词，我们确实感到有些审美疲劳。

（感谢中科院计算所崔翔博士，以及我的同事Billy、Claud、CuteK、纸人、王小花等在选词上的支持）

肖新光

网名江海客，安天实验室首席技术架构师，研究方向为反病毒和计算机犯罪取证等。
新浪微博：weibo.com/seak