寒春：2013年 2月的RSAConference与硅谷

文 / 江海客

APT大背景

RSA Conference作为全球最大的信息安全技术展会，为整个安全业界瞩目。2013年是我们第三次参加这个会议。

为了更多地进行交流，我们决定在RSA Conference开幕前一周到达硅谷。此时却正好遇到Mandiant公司发布了那篇引发全球震动的名为《APT1：Exposing One of China’s Cyber Espionage Units》的报告。这自然成了我们在美国期间经常被询问的话题——另一个参会的国内学者说，他去拜访朋友，朋友家的保姆居然询问起类似话题。

RSA大会前一天，我们参加了另一个安全技术会议BSides SF。Mandiant公司也来发表演讲，题目就叫做《Chinese Advanced Persistent Threats》，通篇基本没有任何技术内容，完全是在“讲政治”。从BSides系列会议的历史来看，这种内容不太可能登堂入室，可见“中国网络威胁”气息之重。

RSA大会期间也充满了浓郁的“类似”气息。我的同事遭遇过几次这样的情况，演示者看到是中国人在观看，就终止了演示，或者拒绝交流。但这种情况在前两届都没有出现。

即便从会议的签名赠书和书店里也能感到这样的味道：例如《Hacking Exposed 7：Network Security Secrets & Solutions》这本书封面被重新贴上了“Hacking Exposed The PLA”的标签来发放；书店里另外一本薄薄的名为《21st Century Chinese Cyberwarfare》的书，以70美元的高价销售着。

在美国期间，媒体和舆论基本上一边倒，没有任何来自中国方面的声音。反而是在RSA大会的主题报告中，信息安全泰斗Adi Shamir，也就是RSA三个作者中的S，发表了唯一一段看起来相对中立的声音：“一个美国的公司这几天发布了一个xx页的报告，说在中国上海有一个大楼，里面有XXX人从网络上入侵了美国；那么过几天就可能有一个中国公司也发一个XX页的报告，在美国也有一个大楼，里面有多少人从网络上入侵了中国。”对于见多识广的老先生来说，含义很简单，既然都彼此彼此，嚷嚷有什么意义。

这篇报告出炉后不久，美国军费预算尘埃落定，军费虽然削减，但网军经费不降反升。

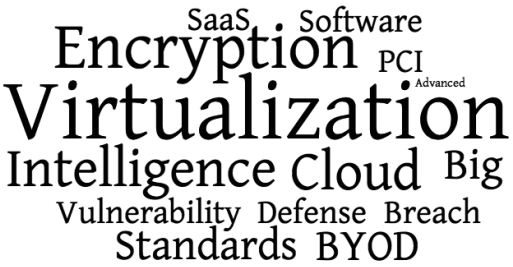
作为一个传统的反病毒工作者，在APT方向上，我们此前一直重点关注Stuxnet、Duqu、Flame这组蠕虫。从破坏铀离心机运行这种事件的级别来看，我们认为这才是Cyber War实战的起始。无疑，美国是这一系列事件的重要嫌疑人之一（另一个是以色列）。而在这种背景下，美国不仅在之前的行为上几乎没有遭到任何谴责，而且能够做到理直气壮地指责中国，并非常有效的占据了全球舆论的高点，其战略之成熟、对国际生态影响之全面，可见一斑。

从网络上我检索到这样一则信息：一个美国官员表达了这样的观点，大意是，“美国情报机构也通过网络获取情报，但我们不会把空客的信息提供给波音。”从这个角度上看，这或许是美国对于网络秩序、交战原则和潜规则的一种诉求和表达。

热点、明星企业：

每年RSA Conference都有一个名为“创新沙盒”的创新创业比赛。2013年的比赛现场，RSA大会执行主席Herbert Hugh Thompson在演讲中总结了安全行业历年的关键词。然而，他发现，在后来真正壮

大的技术和市场，反而是当时不被关注的：



FireEye毫无疑问是2013年RSA大会最为炙手可热的明星企业，这与其反APT标尺企业的身份有关。两年前，FireEye的展台很小，对技术方案的披露谨慎保守，我们只知道它把传统的流量box直接与前置的虚拟机分析结合在一起；2012年的FireEye风头已经显露，但依然有些神秘；2013年的FireEye则比较开放，不仅发布了产品手册，还在把展台三分之二的面积变成宣讲厅，连续进行方案的介绍和讲解。

曾有很多传统反病毒工作者质疑，如果缺乏传统反病毒引擎提供很强的已知恶意代码检测能力，以沙箱（sandbox）为主的单一动态解决方案，能有多大的用处？

但从近两年的观察来看，对于类似方案的价值我有了更多的认识：

1、沙箱解决方案确实对于格式溢出漏洞利用的检测具有先天的优势。不仅因为这种方式确实可以发现未知的漏洞，同时由于格式溢出的手段有限，反虚拟机、反跟踪等技术无法做到PE样本一样灵活，所以用沙箱的成功率较高。

2、美国企业IT网络的治理能力非常强，其网络内部本身安全事件较少，因此一旦发现安全事件就有可能是严重事件。反之，像国内这样中毒频繁，高危险的事件易于被淹没。

移动无线安全是2013年的热点，BYOD炙手可热，相比之下看起来MDM有点像一切中间概念，未熟先老了。

与Windows各安全厂商比拼内核能力相比，Android系统并不开放底层给安全厂商，但安全厂商依然在寻觅解决方案，例如通过VPN的方式取代传统的驱动层Firewall。安全厂商总是能找到在OS场景中存在的位置。这也是一种顽强。

我们还能看到互联网模式也在驱动很多传统领域的变革。例如一家做APP保护的团队提供的是在线加密的解决方案，而不像传统的PC软件保护企业一样销售本地的软件狗、加壳工具等。

企业互动、产业联盟

作为一个传统的网络和移动反病毒引擎厂商，我们来硅谷主要的使命还是寻找新的用户。而我们每次拜访当地的企业都被遇到的一个问题：你们的引擎部署在VirusTotal上么？

第一次面对这个问题时，我不免脸红。因为由于接口问题，我们在VirusTotal的病毒库很长时间无法更新，从而几乎无法检出，而手机检测引擎我们更没打算向其中整合。

当我说明这个问题时，得到的回答反而是：这很好，这样我们才有合作的可能，如果你们的引擎已在VirusTotal上，对我们就没有意义了。细问之后我才知道，硅谷主流的安全企业几乎都购买了VirusTotal最高级别的账户，大家把它当做一个可信资源来使用。这与我们的思路确实有很大的不同——国内一些企业为了保证样本的独家性，是不愿意用VirusTotal做恶意代码检测的。从这个例子也可以看出美国企业间见互信和互动的基础。

当然竞争也是存在的，例如一些厂商都谈及FireEye的崛起对它们的压力。但从展会上看到的信息是，FireEye和这些竞争厂商都选择同一个企业的白名单鉴定服务，这就是2013年另一个热点厂商Bit9，它主要提供高质量的白名单解决方案。我们也去观摩了SOLERA的SOC产品，它对从老牌的Netscreen到新兴的Palo Alto Networks、FireEye等厂商的日志都能够进行综合的分析和管理。

硅谷安全企业并不追求面面俱到，不追求大集成者的位置，它们建立自己的企业个性和强点，创造自己不可替代的独特价值的话语权，而在有其他需求时寻找其他有个性的厂商进行合作。

硅谷生态

创业和并购是硅谷迭代生息的重要生态。因此RSA大会的创新沙盒也甚为业界关注。这是一个安全

领域的创业比赛，参赛者通过选拔，最终在展会期间登坛说法，获得名次和投资。

本次创新沙盒，继续由深厚的硅谷主流企业从业背景的创业者引领。我的两个同事连续旁听了这两届沙盒，对本届沙盒的参赛公司评价不如2012年高。但依然能感受到硅谷的创业文化和对创业者高度宽容——评委们帮助选手积极的寻找着亮点。

我们去年交流过的一个动态分析解决方案的公司，2013年被McAfee以1400万美元的价格收购了。据说国内有企业也参与了竞购，但出价只有McAfee的一半而宣告失败。我曾经奇怪，对于McAfee这样的老牌反病毒企业来说，动态分析本来就是强点，何必再重搞一摊呢？我的同事8w对此分析的十分到位：McAfee作出这样的举动，正是应对FireEye解决方案的竞争压力，采用并购的方式建立新的产品线，与从原有技术中拆离相比。在舆论和灵活度都具有更多的优势，也更容易被金融市场所看到和理解。

从Netscreen、Fortinet到Palo Alto Networks，再到FireEye，硅谷招牌新锐企业裹挟资本力量持续崛起，不断冲击现有格局，形成新的威胁应对和消费热点，成为了美国安全产业与技术的澎湃跌宕的动力。美国成熟的风险投资和资本市场，为新锐企业的崛起，提供了源源不断的动力。而这些新锐公司的压力，也让老牌巨头选择不断收购那些在解决方案上，跟随模仿、微观创新的小公司。这种创业过程，无论是IPO成功还是被并购，都伴生财富和荣誉的过程，极大的活跃了创业与创造的热情。

硅谷企业也是铁打的营盘，流水的兵。但令我惊讶的是完全与国内不同的人才流动的导向，我们认识的一些朋友们，很多都是起步于Netscreen或McAfee，之后他们流向Palo Alto Networks、而今年有的则又在FireEye等新锐创业公司出现了。

来之前已经听说了Berkeley著名华人学者Down Song的一个创业公司被FireEye收购，但没有想到Down Song本人会出现在展台，热忱洋溢地为来宾讲解他们做的APK文件安全分析的演示系统。Down Song老师说她现在比在Berkeley时更加忙碌。让我想起创业时所知道的Palo Alto Networks的工作场景和其他一些硅谷安全公司的创业故事。而与老牌的网络安全企业交流时，感觉到这些工作于大公司的同行更加早九晚五，已把更多精力投入生活和家庭。但他们中的一些人注定不会安于生活，某一定可能会重回“车库”，或者加入某个初创公司，开始新的奇幻漂流。

这种一流人才从大公司到小公司的持续流动是在国内安全界是很难想象的。我曾半开玩笑的对国内某个信息安全管理机构的同仁说，“你们的大规模招聘直插我们专业安全企业的软肋啊。本来中国专业信息安全企业的人才生态就是举步维艰的，后有地下经济的拉拢腐蚀，前有互联网寡头的高薪诱惑，左有出国留校的成长空间，现在右面又多了你们的公务员待遇的吸引。”

或许与APT这种不信任、也具有不可抗力的大背景相比，我更无法不思考的是国内的产业生态。

结束语

如果说中小企业才是活力和创造力、是社会经济的基本基石和标尺这一点已不会为主流经济学界否认的话，那么相比硅谷的企业明星们，中国这些独立而羸弱专业的信息安全企业，未来的命运又将如何呢？

回国后数日，正值《2012年我国互联网网络安全态势综述》发布，其中所能看到的正是危机四伏、潜流纵横，中国从社会运行到民众生活，距离建立起真正的信息安全保障，还任重道远。我们不怕道远路险，但重要的是要知道路在何方？

我透过办公室的窗口，看到北京近期不多的蓝天，也叩问了自己不曾迷失的信念：

坚信，独立信息安全企业的集体崛起，才是一个国家信息安全产业的希望；而每个公民个体获得充分的信息安全保障，才是一个国家信息安全最重要的基石。

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