

## Flashsky 访谈

By flashsky

问：您对桌面安全软件（杀毒软件、主动防御类软件）的前景有什么看法？

答：

- a. 在现有计算机体系结构改进之前，病毒/木马的威胁是长期存在不会消亡的
- b. 但由于操作系统的安全改进，病毒/木马靠漏洞大规模传播的路径将减少，实质威胁会降低，  
导致纯杀毒软件的市场需求会降低
- c. PC 病毒趋势是向应用化（捆绑应用或自身更象应用发展），预装化（捆绑盗版操作系统）发展
- d. 杀毒软件、主动防御类软件需要改进，应对未来的趋势。

问：Windows7 发布后，对安全的影响有哪些？

答：

WINDOWS 7 发布，对安全行业的影响巨大。当然，还得看 WIN7 的普及速度。主要影响：

a. 漏洞挖掘和漏洞利用相关的研究领域，漏洞和漏洞可利用性的减少，相关研究领域要么能突破技术瓶颈，

要么能找到更好的研究成果的利用方式。我个人比较看好和测试方向的结合，实现可度量的软件安全性测试。

b. 以漏洞为基础的整体攻防产业链，未来的攻防，系统漏洞将逐步降低比例，整个漏洞也会演变成攻防中的

一个重要组成而不象现在漏洞是唯一的技术手段，。因此整个产业链都涉及到技术整合和变革中。

c. 新兴的平台或应用：特别是 MOBILE 设备，随着发展，MOBILE 设备的接入方便性，信息资产都会接近现在的

PC，而针对安全漏洞的防护相对当今 PC 要脆弱很多。另外就是硬件设备，特别是在物联网兴起后。

问：请问您认为智能手机操作系统安全与 pc 操作系统安全有何异同？

答：

本质上并无不同，但是有些特性

a. 智能手机目前还无法做到实时打补丁，相对漏洞的时间窗口会很长

b. 目前应用还比较少，所包含的攻击者容易变现的信息资产还比较少，应用和 3G 上网也还没形成气候，攻击者

发起攻击和攻击后植入木马还有困难，所以目前针对手机的地下产业链还未形成，但是未来，应该是继 PC 之后，

地下产业链最主要的舞台。因为手机本身也是支付的手段之一，攻击者攻占一台手机后，相对 PC 又更容易

获取变现的金钱。

c. 智能手机平台相对 PC 更多更杂乱一些，相关攻击的技术方法也还在进一步的研究中。

问：请问您如何看待 SDL？

答：

- a. SDL 是软件工程的重大进步，通过微软的成功实践，证明即使对一个很大的软件工程，通过 SDL，也能非常有效的改善软件的安全。
- b. 未来，普遍使用的软件，以及用于重要场合的软件，都会也应该逐步采用 SDL 过程。
- c. 国内的软件厂商，特别是给国家，重要部门开发使用，以及广泛使用的软件，应该加紧学习 SDL 并将其应用到软件开发过程中。

问：请问您认为中国安全行业和国外安全行业相比有什么异同？

答：

视角更具备前瞻性

在 VISTA 推出之前，SYMANTEC 就实施了大的转型。SYMANTEC 是家非常独特的公司，最先他做 C 的编译器，做的

很好，但是微软一开发 VC，他就立马推出，进军安全产业，留守的 BORLAND 后果如何大家也看到了，而 SYMANTEC

靠进军安全行业，成为全球最大的安全公司，握有的现金流在 IT 公司里也是排名前几的。这次 SYMANTEC 看到

微软改善操作系统安全，实施的转型，其实是一次对安全行业发展的预判。

对比的是 MCAFEE，MCAFEE 坚守安全业务，但是 MCAFEE 也是在 VISTA 出来之初步，重新整合其安全业务，个人觉得，

未来 MCAFEE 针对个人保护的方向是在 WEB 信誉评估，隐私保护等这些更外延的安全上。

问：请问您认为在安全行业自主创业必须具备哪些条件？

答：

- a. 国内创业并不容易：至少需要以下当中的一个：技术，把握一定的客户或者具备销售能力，人脉或者

说关系，资金。其中技术是需要其他至少 1 个因素支撑的因素，如果没有其他因素的支持，除非你的技术

能保证你领先对手很多而客户的需求在相当长一段时间里只有你一家能够满足，否则很容易失败。

- b. 具备了以上 4 个要素中的 2 个(至少 1 个半吧)，你可以去创业了，但是还需要

一个团队：需要你的领导力，说服力，以及看人才的眼光，以及几个合得来有特长的核心伙伴

毅力：创业一般有 3-5 年的困难期，这期间你可能低工资甚至没有工资，还要天天顶着倒闭的压力。

眼光：安全行业是一个变化特别快的行业，变化快说明可选择的方向多，但是把握不好就死的更快，而

创业公司资源有限，如何选择适合自己的方向，同时是可以长期发展的方向，是一个非常困难的事情。

问：请问您在创业过程中遇到的主要困难有哪些？

答：

a. 创新的矛盾：创新后需要培育市场，创业公司资源少，等到市场培育起来，竞争对手满地都是。

b. 客户认同的问题：创业公司都是从小开始，但是需要创新技术的客户都是大客户，他们考虑问题并不单纯

是技术，包括公司整体的实力以及责任等，小公司即使技术第一，也难以获得客户的认同。

c. 资源和机会的矛盾：创业公司，每个机会都需要去争取，但是争取机会也需要消耗资源。对于资源有限的

创业公司，判断和选择是非常困难的。

d. 抉择方向与坚持方向

问：请问您个人下阶段的发展方向是什么？

答：

其实，每个转型都是痛苦的，也是快乐的。痛苦在于，需要不断的学习，并且抛弃一些以前视为很重要的

东西，快乐在于，能让自己理解以前很多不懂的东西。

a. 目前是，做好当前的公司，并把很多创新的技术带入进来，坚持以创新的技术为本，并提升自己对

技术/行业发展方向的判断力。

b. 未来，其实没有预设的人生，比如我从做大型 MIS 系统的系统分析员转入做安全研究人员，也就一个月决定

了的事情，相关积累够了，转向相关的领域，做什么都可以，视情况而定。

问：请您给想从事安全行业的大学生一些建议。

答：

a. 第一是兴趣，没有兴趣，事倍功半，有兴趣，事半功倍

b. 第二是打好技术基础，即使只做销售，技术基础是理解一个行业，发展以及你说服客户的重要基础。

c. 第三是遵守道德和法律，记住自己是一名安全从业人员，而不是黑客。