黑客开发蓝色药丸程序专门对付Vista系统 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/142/2021_2022__E9_BB_91_E5_AE_A2_E5_BC_80_E5_c102_142968.htm 据国外媒体报道，黑客程序研究人员一直在开发一款名为“ 蓝色药丸 ”的程序，并以该程序为基础编写微软下一代操作系统Windows Vista所不能发现的恶意程序，预计该隐形恶意程序将于数月内完工。 据一家英国网站报道，现供职于新加坡电脑安全行动顾问公司的波兰黑客程序专家乔纳鲁科维斯基，今年早些时候演示了一款蓝色药丸程序原型。在马来西亚吉隆坡举行的黑客安全大会（HITB）上接受采访时鲁科维斯基表示：“ 所谓的蓝色药丸，就是劫持一个操作系统，并进入虚拟机，从而对其进行控制。 ”蓝色药丸程序之所以得逞，其实主要利用了AMD和英特尔处理器中使用的硬件虚拟技术，由于使用了虚拟技术，电脑硬盘的不同分区可以同时运行完全不同的操作系统。“ 借助于这种虚拟技术提供的便利，我们可以开发出完全隐蔽的恶意程序。 ”鲁科维斯基表示。她表示，今年初演示的蓝色药丸基本可达到预定目标，但电脑在启动一操作系统时的系统时间自检过程中，理论上也可发现蓝色药丸是否存在，目前，她正潜心研究一款使用同样方法入侵后完全隐蔽的蓝色药丸程序。 防御蓝色药丸程序侵入的最佳方法是关闭处理器的虚拟化功能，但这势必遭到芯片厂商的强烈反对。“ 研究人员花费数年时间才开发出了具备虚拟功能的新型处理器，现在却要关闭这些功能，这合适吗？显然不符合常理。 ”鲁科维斯基表示。相比之下，目前比较可行的办法是要求微软将Vista操作系统内核内存的分页功能关闭，也

就就是说将大约80MB的内核代码和驱动程序上载到主存中，这样可阻止蓝色药丸进入内核并执行代码。鲁科维斯基表示，“ 80MB内存算得了什么？但令人奇怪的是，我7月底在SysCan大会上演示了类似攻击后，至今微软仍没有对RC1做出任何修改。 ”RC1即微软最新的、打算交付量产的Vista产品。 微软也对上述说法作出了回应，公司一位安全专家表示，在Vista RC1交付用户之前，公司仍将不断提高其安全性能。微软安全应急中心运营经理迈克鲁维表示，“ Vista 最终版本推出尚有几个月时间，其安全性能仍处于完善中。 ”