

熊猫烧香：噩梦已过还是刚刚开始 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/139/2021\\_2022\\_\\_E7\\_86\\_8A\\_E7\\_8C\\_AB\\_E7\\_83\\_A7\\_E9\\_c100\\_139482.htm](https://www.100test.com/kao_ti2020/139/2021_2022__E7_86_8A_E7_8C_AB_E7_83_A7_E9_c100_139482.htm) “熊猫烧香”考问网络安全 京华时报1月26日报道 这是一波电脑病毒蔓延的狂潮。在两个多月的时间里，数百万电脑用户被卷将进去，那只憨态可掬、颌首敬香的“熊猫”除而不尽，成为人们噩梦般的记忆。反病毒工程师们将它命名为“尼姆亚”。它还有一个更通俗的名字“熊猫烧香”。它迅速化身数百种，不断入侵个人电脑，感染门户网站，击溃企业数据系统……它的蔓延考问着网络的公共安全，同时引发了一场虚拟世界里“道”与“魔”的较量。反病毒工程师和民间反病毒人士纷纷投身其中。1月19日，一个最新的“熊猫烧香”变种病毒出现。病毒作者宣称，这将是“熊猫烧香”最后一次更新。这场历时两个多月的较量结束了吗？“蜜罐”中发现病毒 2006年11月14日，中关村瑞星公司总部14楼。一群反病毒工程师围着一台与网络隔绝的电脑。随着鼠标点动，数百个熊猫图标出现在屏幕上。这是工程师们当天捕获的病毒，命名为“尼姆亚”。史是瑞星公司研发部病毒组的反病毒工程师。他每天的工作就是，和数十名伙伴一起捕捉网上流传的病毒，然后将病毒“拆”开，研究其内部结构后，升级瑞星的病毒库。当天下午，一名用户向他们提交了一份病毒样本。随后，他们又在病毒组的“蜜罐”内，发现了该病毒的踪影。“蜜罐”是病毒组设立在互联网上的一些防卫性孱弱的服务器，工程师们故意在服务器上设置多种漏洞，诱使病毒侵入。“就像猎人做的沾满蜜糖的陷阱，专门吸引猎物上钩。”从“蜜

罐”里提取病毒后，史和同事们将病毒移到公司14楼的一台与网络隔离的电脑上，这里是病毒的“解剖台”。“运行病毒之后，系统所有的图标都变成了熊猫。”史眼前的屏幕上，出现了一排排的熊猫图案，熊猫们手持三炷香，合十作揖。经过分析，工程师们发现，在病毒卡通化的外表下，隐藏着巨大的传染潜力，它的传染模式和杀伤手段，与风行一时的“威金”病毒十分相像。瑞星公司随即发布病毒预警。反毒人员在“解剖”病毒后，发现里面的留言。本报记者刘军摄熊猫烧香病毒表情/资料图片病毒蔓延涌向全国“最开始的‘尼姆亚’不算厉害。”史说，随着病毒作者的不断更新，它的破坏力和传染力也随之上升。2006年11月底，“尼姆亚”只有不到十个变种，然而12月开始，病毒作者从数日一更新，变为一日数更新，它的变种数量成倍上升。这时候，“熊猫烧香”已经取代了“尼姆亚”这个名字。12月中旬，“熊猫烧香”进入急速变种期，在几次大面积暴发之后，“熊猫烧香”成为众多电脑用户谈之色变的词汇。圣诞节过后，“熊猫烧香”版本已达到近百个。史说，去年12月下旬，国内近千家大型企业感染“熊猫烧香”，向瑞星求助。“当病毒变种和感染人群超过一定数量时，病毒的传播就会以几何方式增长。”12月26日，金山毒霸全球反病毒监测中心发布“熊猫烧香”正疯狂作案的病毒预警。27日，江民科技发布关于“熊猫烧香”的紧急病毒警报。2007年1月7日，国家计算机病毒应急处理中心紧急预警，“通过对互联网络的监测发现，一伪装成‘熊猫烧香’图案的蠕虫病毒传播，已有很多企业局域网遭受该蠕虫的感染。”1月9日，“熊猫烧香”继续蔓延，开始向全国范围的电脑用户涌去。这一天，“

“熊猫烧香”迎来了一次全国性的大规模暴发，它的变种数量定格在306个。各地用户纷纷中招。小江是黑龙江省一家网吧的网管。1月9日到1月10日的两天间，他所在的网吧内空空荡荡，并无顾客，打开网吧的40多台电脑，屏幕上布满了“熊猫烧香”图标，系统崩溃，无法运行。“毒是9日早晨中的，一开始只是一台机器，我杀毒时候，局域网内其他机器陆续中招。”小江说。同一天早晨，在北京一家IT公司工作的刘先生上班后发现，公司近30台电脑全部感染“熊猫烧香”，病毒破坏了电脑内的程序文件，并删除了电脑备份，公司正在研发中的半成品软件毁于一旦。刘先生愤怒之下却又无奈。在年度总结报告中，他特意加上了一条：“以后重要程序必须备份，防范类似‘熊猫烧香’的流氓病毒。”同一天晚上，北京的一家报社里，技术人员们东奔西跑，几十名编辑记者都在等待着他们清除电脑里的“熊猫烧香”。1月10日，上海一家台资公司的员工张先生打开电脑，迎接他的是一排排拱手举香的熊猫。环顾四周，他发现同事们脸上有同样的惊诧表情。整整一天，公司业务陷于瘫痪。……根据瑞星公司提供的“熊猫烧香”病毒用户求助数据，仅1月9日一天，瑞星用户向公司求助的人数已达1016人次，11日达到1002人次。因为是选择性求助，并仅限于瑞星杀毒软件的正版用户，这个数据只是冰山一角。据了解，1月9日感染的电脑用户达数十万。其中北京、上海等电脑用户较集中的城市成为“重灾区”。100Test 下载频道开通，各类考试题目直接下载。详细请访问 [www.100test.com](http://www.100test.com)