War

不流血的战争

网络攻防经典之战

樊高月　赵力昌　主编

解放军出版社

不流血的战争

网络攻防经典之战

樊高月　赵力昌　主编

解放军出版社

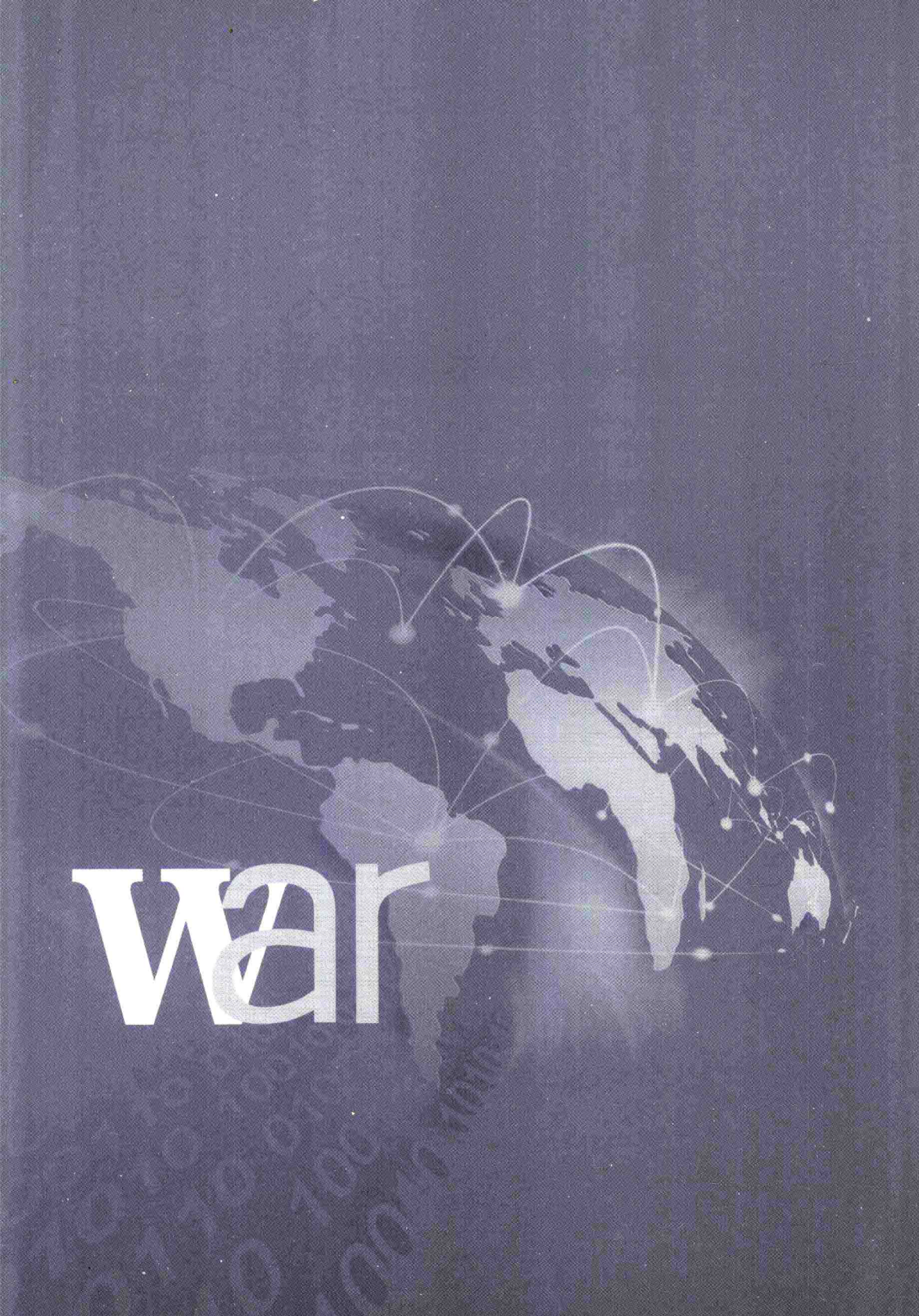
图书在版编目(CIP)数据

不流血的战争:网络攻防经典之战 / 樊高月编著.
—北京:解放军出版社,2014.3
ISBN 978-7-5065-6760-2

Ⅰ.①不… Ⅱ.①樊… Ⅲ.①计算机网络—应用—战争
Ⅳ.①E919

中国版本图书馆 CIP 数据核字(2014)第 000964 号

书　　名：不流血的战争——网络攻防经典之战
作　　者：樊高月　赵力昌
责任编辑：王世光
出版发行：解放军出版社
社　　址：北京市西城区地安门西大街 40 号　邮编：100035
电　　话：010－66531659
E－mail：jfjcbs@126.com
经　　销：全国新华书店
印　　刷：北京中科印刷有限公司
开　　本：700 毫米×1000 毫米　1/16
字　　数：269 千
印　　张：17.5
版　　次：2014 年 3 月第 1 版
印　　次：2014 年 3 月北京第 1 次印刷
书　　号：ISBN 978-7-5065-6760-2
定　　价：35.00 元
(如有印刷、装订错误，请寄本社发行部调换)


war

前 言

一提起战争，人们便习惯地联想到炮声隆隆、硝烟弥漫、弹片横飞、尸横遍野、血流成河的战争场面。然而，信息时代发生在互联网上的战争却以一般人意想不到的形态悄然降临：无人、无声、无形，没有刀光剑影，没有枪林弹雨，没有血流成河。2003年3月，美军在开始常规攻击之前，侵入伊军专用军事保密网络，向数以千计的伊军军官发送电子邮件，劝其将坦克和其他装甲车辆整齐地停放在基地外面并远离它们，获得成功，致使伊军部队未经交战就消失得无影无踪。2007年9月6日深夜，以色列战机通过发动网络攻击骗过叙利亚防空网，毫发无损地摧毁了叙利亚境内的“核设施”。2008年8月7日，俄罗斯与格鲁吉亚发生冲突，俄对格实施了持续、复杂和高强度的网络攻击，致使格鲁吉亚丧失对本国“.ge”域名的控制权，被迫将许多政府网站转移到国外的服务器上，但俄随即改变攻击路径，假装是来自格鲁吉亚的网络攻击，结果触发了多数国外银行的自动保护机制，关闭了它们与格鲁吉亚银行的连接，致使格银行因无法访问欧洲的结算系统而业务瘫痪，不但信用卡系统停止工作，移动电话系统也随即崩溃。

为了进行这种新型战争，美军1995年就已培养出第一批16名专门以计算机为武器的“网络战士”，2002年组建了网络与空间作战司令部，2006年组建了第一支网络战部队，2009年组建了隶属于战略司令部的“美国网络司令部”(U.S.Cyber Command)，专门负责指挥美军网空作战部

队保护五角大楼全球网络系统和对敌发动网络攻击。与此同时，美军投入大量资源研究“网络基因”、“网络电磁实物系统”等网空作战武器，开发网空作战理论，建设网空作战训练设施，并于2011年11月首次举行代号为“网旗12-1”的联合网络对抗演习。俄、日、英、法、印等国军队也已建立或正在筹建自己的网络战司令部和网空作战部队，为网络攻防作战厉兵秣马，呈现出一派“山雨欲来风满楼”的临战气氛。

然而，网络空间面临的巨大威胁不仅来自各国正规网空作战力量随时可能发动的网络攻击，而且来自网络间谍、黑客入侵、网络犯罪和恶意软件。美国掌控着世界上全部13个互联网根服务器，监管着互联网域名与地址管理公司，网络技术远远领先于其他国家，在网络空间享有完全的行动自由，想获取什么信息就获取什么信息，想监控哪个国家就监控哪个国家，对国际网络空间安全构成最大威胁，美国中央情报局技术人员爱德华·斯诺登披露的“棱镜”计划最充分地说明了这一点。除政府情报部门外，网络黑客的入侵也对网络空间安全构成持续而严重的威胁。《2011年中国互联网络安全态势报告》显示，2011年境外有近4.7万个IP地址参与控制中国境内近890万台主机；境外11851个IP通过植入后门对境内10593个网站实施远程控制。2006年以来，中国网络上的犯罪总量持续高位运行，年平均在470万起以上，其中最突出的问题是色情泛滥成灾，严重危害未成年人的身心健康；软件、影视、唱片的著作权受到盗版行为的严重侵犯，商家损失之大无可估量；网络商务备受诈骗的困扰，有的信用卡被盗刷，有的购买的商品如石沉大海，有的发出商品却收不回货款。“莫里斯”蠕虫、“梅利莎”病毒、“红色代码”病毒、“震网”病毒等恶意软件，通过漏洞侵入、后门植入、硬件注入、接收路径传入等方式，对计算机系统进行破坏，造成难以估量的巨大损失。

但遗憾的是，我国大多数网民（到2013年6月底，我国网站总数升至294万个，域名总数为1470万个，网民规模达到5.91亿，普及率由2005年的8.5%提升至44.1%。）和某些相关部门，对这些看不见、摸不着、来无影、去无踪的网络威胁缺乏应有的警觉，疏于防范，许多应用系统几乎处于不设防状态，给网络安全留下了重大隐患。为应对我国网络空间

安全面临的重大现实威胁，我们于2012年6月1日建立了“网络安全研究小组”，对网络安全的相关问题进行跟踪研究，意在探索加强网络安全的有效方法。为使广大网民了解网络空间面临的重大现实威胁和可能造成的严重危害，增强网络安全意识，加强网络安全防护，我们编写了这本《不流血的战争——网络攻防经典之战》，供大家参考。

本书包括“黑客大战”、“网战实录”、“网战演习”、“网战构想”和“附件”五个部分。“黑客大战”主要描述和分析世界影响较大的黑客人物和黑客事件，揭示黑客犯罪活动的背景和原因。“网战实录”主要描述和分析史无前例的网络攻防行动，揭示网络安全面临的巨大威胁和挑战。“网战演习”主要介绍和分析美国及其盟国进行的网络攻防演练活动，警示人们网络战争即将来临。“网战构想”主要设想和分析网络战争可能发生的时间、地点、进程和危害，呼吁世人未雨绸缪，防止网络战争。“附件”介绍美国网络空间行动战略、外国网络战部队和网络战武器，提醒人们网空领域的竞争可能会愈演愈烈。值得特别关注的是，某些西方国家和别有用心的人大肆炒作“中国黑客威胁”论，污蔑中国政府和军队支持黑客盗取科技情报和工商机密，其根本目的是为了掩盖其侦察监视别国的网络活动，为其组建网络战部队和研发网络战武器正名。

本书由樊高月、赵力昌任主编，肖铁峰、丁卫华、吕晶华任编委。樊高月负责提出创意、设计框架、组织讨论、撰写前言与附件一、二和全书统稿；赵力昌负责部分主编工作、参与讨论并撰写“黑客大战”；吕晶华参与讨论并撰写“网战实录”和附件三；丁卫华参与讨论并撰写“网战演习”；肖铁峰参与讨论并撰写“网战构想”。由于各部分具有相对的独立性，写作风格和体例未作强行统一。由于网络攻防具有高度机密性，公开资料不多，再加之我们能力有限，时间仓促，书中可能存在这样那样的问题，欢迎广大读者批评指正。

编者

2013年9月22日

目　录

黑客大战

网战实录

网战演习

网战构想

黑客大战

少年黑客挑战联邦调查局

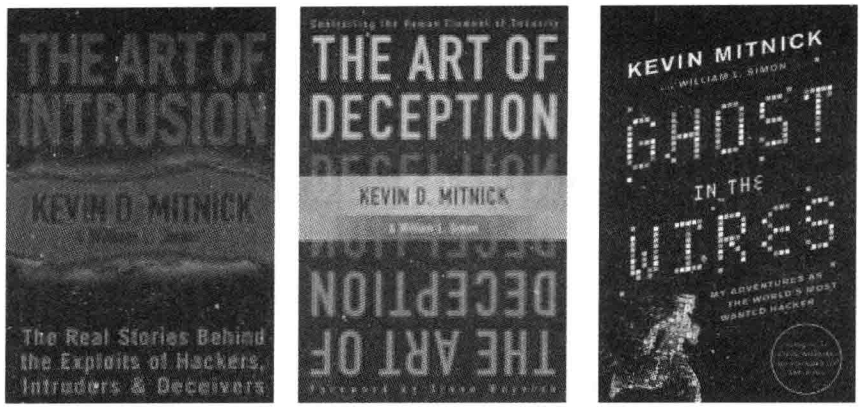
“巡游五角大楼，登录克里姆林宫，进出全球所有计算机系统，摧垮全球金融秩序和重建新的世界格局，谁也阻挡不了我们的进攻，我们才是世界的主宰”

——凯文·米特尼克

好莱坞经典电影“Matrix”（黑客帝国）中有一句非常经典的台词：“Everything that has a beginning has an end”，意为“万物有始必有终”。是的，计算机及网络的出现其实就是代表了工业时代的落幕和信息时代的开始。在信息时代，由于信息的大流通和大丰富，人的视野将变得无限开阔，在工业时代被“异化”的人逐渐成长为“信息化的人”，他们的代表就是“黑客”。

黑客一词现在已经成为一个带有神秘、隐秘、高技术、信息化色彩的词汇，军事学者乔良在其小说《末日之门》中提出“黑客”应该被称为“海客”，因为这样有一种非常海阔天空、自由自在的感觉。一般而言，在稍微技术化的文本中，“黑客(Hacker)”与“骇客(Cracker)”的称谓确实有些分别，前者是以技术性路线发现漏洞，并以神不知鬼不觉的手段“黑进去”，然后再神不知鬼不觉地出来，有时还会给进去的人家留个“善意”的提醒；而后者通常崇尚以暴力破解、海量数据攻击等手段，瘫痪、篡改、盗取信息及其宿主，具有现实上违反法律的行为。通常二者之间的界限是比较模糊的，其实也没必要分得太清，因为他们都是遨游在网络海洋中、搏击数据风浪的网络战士。

本节的主人公凯文·米特尼克就是第一代、甚至可以说是第一个（也是最出名的一个）典型“黑客”，那一年他只有15岁。



米特尼克的著作——《入侵的艺术》、《欺骗的艺术》、《线上幽灵》

崭露头角，入侵防空指挥部

凯文·米特尼克 1963 年 8 月 6 日出生在美国洛杉矶一个中下阶层的家庭里。3 岁时父母就离异了，他跟着母亲劳拉生活。家庭环境的变迁致使他性格十分孤僻，学习成绩也不佳。但实际上他是个极为聪明、喜欢钻研的少年，同时他对自己的能力也颇为欣赏。当米特尼克刚刚接触到电脑时，就已经明白他这一生将与电脑密不可分。他对电脑有一种特殊的感情。电脑语言“0、1”蕴涵的数理逻辑知识与他的思维方式天生合拍，在学习电脑的过程中，米特尼克几乎没有遇到过什么太大的障碍。他编写的程序简洁、实用、所表现的美感令电脑教师都为之倾倒。他的电脑知识很快便超出了他的年龄。

在 15 岁的时候，米特尼克盯上了北美防空司令部，他尝试仅凭一台电脑和一部调制解调器能否入侵计算机系统主机，同时还能悄然无息地溜出来。在破解密码的过程中，米特尼克一开始就碰到了极为棘手的问题，毕竟事关整个北美地区的安全，这套系统的密码设置非常复杂，米特尼克最初设计的解码程序很快就败下阵来。但是米特尼克喜欢挑战，他用了两个月时间升级他的解码程序，最后终于找到了北美防空司令部的“后门”，这正是整套系统的薄弱环节，也是软件的设计者留下来以方便自己进入系统的地方（按照软件系统的开发规范，这样的“后门”允许在开发调试阶段存在，因为

程序员毕竟需要一些较为便捷的方式对程序进行调试，但是一旦软件开发进入最终用户阶段，即所谓的 α 版，这些后门必须要从系统中消除）。通过“走后门”，米特尼克顺顺当当，“大摇大摆”地进入了这个系统。他向身边的朋友们吹嘘：“我知道美国所有指向天空，指向俄国及其盟友的核导弹的名称、数量和位置！”同伴们不相信，他就打开电脑，让他们开开眼界。小伙伴们终于相信米特尼克说的是真的，一个个都目瞪口呆，对他当然都佩服得五体投地。对此，米特尼克心理上非常满足。同伴们将他们的特大发现告诉大人，当时没有人相信这些孩子说的是真话。

他成功了，这次入侵成为了黑客历史上一次经典之作，也成为美国军方的一大丑闻。后来美国核安全专家对他可能造成的损失做了如下估计：如果米特尼克把这些情报卖给前苏联情报人员的话，至少将获得 50 万美元，而美国至少要花几十亿美元的重新部署、修改程序的费用，才能弥补这一损失（请注意这是 1978 年）。1983 年好莱坞曾以此为蓝本，拍摄了电影《战争游戏》，演绎了一个同样的故事（在电影中一个少年黑客几乎引发了第三次世界大战）。

首次被捕，结“缘”联邦调查局

故事要从 20 世纪 80 年代初说起。这时米特尼克已经 18 岁了，他已经掌握了用远程方式轻而易举地进入电话公司电脑的方法，使他可以任意地拨打免费电话，还可以随意偷听任何人的电话。1981 年，米特尼克和同伙在某个假日潜入“太平洋电话公司”洛杉矶电话中心盗取了一批用户密码，毁掉了其中央控制电脑内的一些档案，并用假名植入了一批可供他们使用的电话号码。这次事件闹得很大，不久电话公司便发现了并向警察局报案，警方进行了周密地调查可始终没有结果，而这就引起了联邦调查局的注意。

比较有意思的是，米特尼克这时也对联邦调查局的电脑产生了“兴趣”，经过一番攻击成功进入其中，在其中他发现某份文件中显示联邦调查局正在调查一名黑客，打开文件一看原来要调查的就是他自己，但是米特尼克对此不屑一顾，潜台词无外乎“就你们这水平还调查我呢？”但天网恢恢，有一天一名米特尼克同伙的女朋友向警方举报，这时才真相大白。也许由于当时米特尼克年纪尚小，17 岁的米特尼克只被判监禁 3 个月，外加一年监视

居住。老师们赞叹他是一位电脑奇才，认为他是个很有培养前途的天才少年，由于只有十几岁，但网络犯罪行为不断，所以他被人称为是"迷失在网络世界的小男孩"。但首次监狱生活不仅未使他改过自新，反而使他变本加厉地在网络黑客的道路上越走越远。

1983年，米特尼克使用一台大学里的电脑进入今日互联网的前身ARPA网，并通过该网进入了美国五角大楼的电脑。这次他很快就被发现，被判在加州的青年管教所管教了6个月。被释放后，米特尼克干脆申请了一个号码为"XHACKER"即"前黑客"的汽车牌照，挂在自己的尼桑车上。此后，米特尼克继续在网络上横行无忌，时而潜入软件公司非法窃取其软件，时而进入电脑研究机构的实验室制造麻烦，并继续给电话公司捣蛋。

1988年他再次被执法当局逮捕，原因是：DEC指控他从公司网络上盗取了价值100万美元的软件，并造成了400万美元损失。这次，他甚至未被允许保释，心有余悸的警察当局甚至认为，他只要拥有键盘就会对社会构成威胁。这其实并不夸张，很多电影里都有这样的情节，一名电脑高手把键盘接在提款机（或公用电话，或摄像头）线路上，一番折腾就能进入银行（或军事基地）内部网络。米特尼克被判处一年徒刑。一年之后，他又施展绝技，成功地侵入了几家世界知名高科技公司的电脑系统。根据这些公司的报案资料，联邦调查局推算它们的损失共达3亿美元。正当警方准备再度将之逮捕时，米特尼克突然从住所消失，过起了逃亡的地下生活。

于是，他被联邦调查局通缉，成为在FBI"悬赏捉拿"海报上第一个露面的黑客。然而米特尼克不愧为"不世出的高手"，在逃亡过程中，还顺便入侵了加州当地的电话系统网络，从而能够窃听追捕他的警探的电话。


WANTED
BY U.S. MARSHALS
NOTICE TO ARRESTING AGENCY Before arrest, validate warrant through National Crime Information Center (NCIC).
United States Marshals Service NCIC entry number: (NIC/ W321440021).
NAME: .....MITNICK, KEVIN DAVID
AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN
DESCRIPTION:
Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Build: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number (s): 550-79-5495
NCIC Fingerprint Classification: DOPM20PM13DIPM199409

FBI对米特尼克的通缉令海报

魔消道长，凯文对决下村勉

《苏菲的世界》中有一句话“要成为一名哲学家，首要的、也是唯一的条件，就是要有好奇心”，这一条几乎对所有的黑客都适用。就算身处被通缉的境地，米特尼克仍然没有放弃对未知的探索，追寻挑战权威的快感。

1994年圣诞节，米特尼克向圣迭戈超级计算机中心发动了一次攻击，《纽约时报》称这一行为“将整个互联网置于一种危险的境地”。这一攻击的对象中还包括一个因为米特尼克而成名的人物，即后来人称“美国最出色的电脑安全专家之一”、在该中心工作的日裔美籍计算机专家下村勉。他在向下村发出事前警告之后，入侵了下村勉家里的计算机，盗窃出对付“黑客”的软件，并留言声称：“还是我高明。”

1995年2月15日，下村勉历尽千辛万苦终于发现了米特尼克的行踪——藏匿在北卡罗来纳州的一个小镇，并迅速通知美国联邦调查局将这个被称为“最出色的网络窃贼”、“地狱黑客”的米特尼克逮捕。1995年2月，米特尼克终于被送上了法庭。在法庭上，戴着手铐的米特尼克转向第一次见面并出庭作证的下村，由衷地说：“你好啊下村，我钦佩你的技术”。这次，他被指控犯有23项罪，后又增加25项附加罪。

面临审判，全球黑客大声援

1997年12月8日，米特尼克的网络支持者要求美国政府释放米特尼克，否则，他们将启动已经通过网络植入世界许多电脑中的病毒！他们宣称，一旦米特尼克获释，他们将提供病毒的破解方法。一时间，因特网又陷入了一次新的恐慌之中。在当时全球最著名的网站雅虎(YAHOO！)网页上，这批自称PANTS、HAGIS的身份不明的网络黑客留下了一则勒索便条。这张便条声称，他们在雅虎网页上放置了逻辑炸弹，过去一个月里凡是浏览过雅虎网站的电脑均被植入了病毒。这种病毒的逻辑炸弹将于1998年圣诞节启动，在全球电脑网络中四处肆虐。他们宣称，一旦米特尼克获释，他们将提供病毒的破解法。这件事足以证明米特尼克在黑客中的地位。

在狱中，米特尼克也没有消停，他自己改造了一台不知从哪儿弄到手的AFFM收音机，并试着用它来监听监狱管理人员的谈话，为此他被监狱当局从普通牢房转到隔离牢房，实行24小时连续监管。

审判一直进行到1999年3月16日，米特尼克承认其中5项罪名和两项附加罪，总共被判刑68个月，外加3年监督居住。联邦调查局还指控他造成了几亿美元的损失，控方要求的赔偿额是150万美元。据说，米特尼克的侵入行为导致他们蒙受大约2亿9000万美元的损失。这些受害者包括高科技大公司如Sun系统公司、Novell电脑公司、NEC美国公司、诺基亚公司等。律师在为他辩护时称，“黑客行为犹如吸毒，靠当事人的理智绝对无法改变这一行为。”米特尼克一心扑在电脑上，黑客行为使他感到兴奋不已。

凯文出狱，第一黑客金盆洗手

2000年1月21日，美国法庭宣布米特尼克假释出狱。此时他的身体比过去略瘦，但显得更加精悍。媒体广泛报道了他被释放的消息，提到他打算“先上大学重新学习电脑”。可他的愿望大概很难实现，当局将在今后三年对米特尼克(36岁)实施缓刑。在此期间，他不允许接触任何数字设备，包括程控电话、手机和任何电脑。因为有关当局担心这位大名鼎鼎的黑客一旦接触到电脑，会再度给互联网世界带来麻烦。

出狱不久，米特尼克得到了一份工作：为一家互联网杂志写专栏文章。但是，法官认为这份工作“不适合于他”，怕他制造破坏计算机、网络系统的技术。米特尼克不认为自己连写文章的权利都没有。为此，他重新走上法庭，要求允许他成为一家因特网杂志的专栏作家。如果如愿以偿地得到这份工作，他将获得每月5000美元左右的底薪，每写一篇文章另外获得750美元的报酬，以及出版物的50%的利润。但他的律师伦道夫说，米特尼克要在大学攻读电脑学科，为此，他准备向当局申请批准使用电脑……米特尼克的所作所为与通常人们所熟悉的犯罪不同，他所做的这一切似乎都不是为了钱，当然也不仅仅是为了报复他人或社会。他作为一个自由的电脑编程人员，用的是旧车，住的也是他母亲的旧公寓。他也并没有利用他在电脑方面公认的天才或利用他的超人技艺去弄钱，尽管这对他并不是十分困难的事。同时他也没有想过利用自己解密进入某些系统后，窃取的重要情报来卖钱。