1.“头号黑客”

凯文·米特尼克，号称“世界头号黑客”，1963 年出生于美国洛杉矶。16 岁时，米特尼克凭借一台电脑和一部调制解调器侵入了北美空中防务指挥部的网络系统，美国国防部、国家税务局、花旗银行……这些防守最严密的网络系统都先后被米特尼克光顾过。名声大噪的同时，米特尼克也成为第一个被美国联邦调查局通缉的黑客。即使上了通缉令，米特尼克也没有任何慌乱，而是设法侵入联邦调查局，准确掌握了围捕他的行动计划，并找出所有参与行动计划的特工的姓名和家庭住址，他还利用联邦调查局的警报系统及时获知拘捕他的行动，并逃之夭夭。

U.S. Department of Justice
United States Marshals Service

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/ W721460021).

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
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS
VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office. (Telephone: 213-894-2485).
If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102 (24 hour telephone contact) NLETS access code is VAUSM0000.

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

Form USM -132
(Rev. 3/2/82)

November 1992

美国司法部法警局缉拿凯文·米特尼克的通缉令

图片来源：美国司法部网站 http://www.justice.gov

美国有一家大型信用卡公司，客户信息是该公司数据库系统的核心资产，为了保障系统安全，公司设置了从技术上到制度上的重重防护，包括多重加密、系统隔离、专业管理、专人值守等措施，公司所在的商务大楼也配备了专业保安和一人一卡的门禁系统。

米特尼克为了侵入该系统，设计了一个周密的计划：

（1）伪造：米特尼克装扮成一名快递员，以向一名公司雇员投递包裹为由，近距离仔细查看员工胸卡字体格式等细节，然后从公司网站下载了公司标识，制作出了几可乱真的胸卡；

（2）尾随：米特尼克跟在一群公司雇员后面，乘前面雇员用胸卡打开自动门禁时，跟随着这群“同事”一并进入公司大门；

（3）潜伏：找到预先查找过的拥有进入公司信用卡数据库系统完整权限的系统工程师的办公室，然后在大楼一角潜伏下来；

（4）入侵：待公司人员下班后，进入系统工程师办公室，使用黑客工具光盘启动工作电脑，修改本地管理员口令，重启电脑，以管理员身份登陆；

（5）植入：安装木马程序，可实现远程控制电脑、监控键盘输入、调用摄像头等功能。

（6）消踪：调用系统注册表，修改键值，消除本次登录及安装木马程序等所有操作记录。

（7）破解：第二天，系统工程师打开电脑，进行信用卡系统维护日常操作，木马程序随之启动，远程连接成功，取得域控制服务器权限，下载存储公司所有用户的账号和口令（密文）的文件，破解口令。

（8）窃密：寻找用于处理客户请求的后端服务器，运行数据库的存储过程，找到信用卡卡号的加密密钥。

（9）收获：公司数百万客户的信用卡信息，卡号、密码、姓名、住址、联系方式，应有尽有。有了这些信息，米特尼克可以随意使用其中任何一张信用卡。

上述环环相扣的攻击手法，每一个环节都利用了这家信用卡公司网络系统的安全漏洞。一些漏洞是通过技术手段发现和利用的，还有一些漏洞涉及到一种“社会工程学”的非技术渗透手段，如门禁系统没有对每个员工都验证胸卡、公司胸

卡和公司网站使用了一致的标识，通过人际交流和社会关系等方式可以获得有助于入侵网络的关键信息和系统漏洞。

米特尼克有着无数次攻击和入侵形形色色、大大小小网络系统的经历，对他而言，那些经过投入重金、精心设计、反复推敲、层层把关的技术措施和管理制度，看上去似乎已经做到了无懈可击、无机可乘，却是处处隐藏足以形成致命一击的漏洞。只要深入分析，结合社会工程学的攻击手段，总是有机会找到突破口。

1. “罗宾汉”与“海盗湾”

亚伦·施瓦茨，1986 年 11 月出生于美国伊利诺伊州，从小痴迷于电脑编程，是一名技术神童。2000 年，施瓦茨开始运用维基技术设计在线百科全书，2001 年，年仅 15 岁的施瓦茨与人合作编写了 RSS1.0 协议规范，这是一种可扩展的元数据描述和同步格式，用来发布经常更新数据的网站。RSS1.0 协议得到万维网联盟（W3C）确认，成为互联网通用规范之一，这使得施瓦茨声名鹊起，成为万维网联盟资源描述框架（W3C RDF）核心工作组最年轻的成员。

高中毕业后，施瓦茨考上了斯坦福大学，但仅读了一年，就退学专注于互联网创业。施瓦茨先后创建了一家软件公司和一个社交新闻网站，2006 年，施瓦茨创办了一个免费在线图书馆，目的是为每一本已经出版的书都建立一个单独的网页。施瓦茨还希望有更大作为，他立志成为“数字时代的罗宾汉”，而施瓦茨劫的“富”，是被联邦政府和商业机构垄断的版权文献，济的“贫”就是广大互联网用户。

美国联邦法院建立了一个庞大的电子资料数据库，面向社会公众开放，但需要阅读者按照内容付费。很多美国网民对此很有意见，他们认为资料库是由政府出资建设的，应该免费供公众阅读。为了以实际行动支持网民诉求，2008 年，施瓦茨侵入联邦法院资料库，一口气下载了二千万页资料，发送到网上供网民免费下载。

施瓦茨紧接着盯上了更有价值的商业数据库，自 2010 年底到 2011 年初，施瓦茨在麻省理工学院的一间机房外，用一台笔记本电脑接入内网，运行了一段自动下载脚本，从电子期刊库 JSTOR 里下载了大约 480 万篇学术论文，监控摄像头记录下了他的所有操作。2011 年 7 月，施瓦茨被捕，联邦检察官对其提出非法侵入计算机系统等 13 项指控，如果罪名成立，施瓦茨将面临最高 35 年监禁。压力之下，施瓦茨选择了自杀，留下诸多感慨。更令人稀嘘不已的是，就在两天前，JSTOR 宣布施瓦茨下载的论文中的至少 450 万篇免费向公众开放。

施瓦茨的反版权行为，与互联网的自由理念密切相关，因为“自由”一词的英文“free”也有免费的意思。最初互联网运营企业以免费吸引用户访问，内容发布者以免费获得关注，久而久之，免费就演化为网络空间的流行文化，成

为一部分人坚决维护的价值观。既然有施瓦茨们坚持免费理念，想方设法拿到版权文献分享给广大网民，那么也就有坚持出版自由的“海盗湾”们，想方设法让网民更方便、更快速地下载这些版权文献。

“海盗湾”是一个非政府组织，2004 年 10 月成立于瑞典。这个组织反对任何形式的版权保护，为了实现真正自由地传播言论和知识，海盗湾进行了不屈不挠的抗争。“海盗湾”搜集了大量受版权保护的电子文档，其中很大一部分来源于用户上传，“海盗湾”专门建立了一个可储存、分类、查询及下载海量电子文档的网站，一度成为世界上最大的免费获取版权文献的基地。

“海盗湾”分发电子文档的主要方式是比特流下载，这是一种内容分发协议，采用高效的点对点传输技术，下载者在下载的同时不断向其他下载者上传数据。文档持有者先将文件发送给其中一名用户，再由这名用户转发给其它用户，用户之间相互转发自己所拥有的文件部分，直到每个用户的下载都全部完成。这种技术可以使下载服务器同时处理多个大体积文件的下载请求，而无须占用大量带宽，而且用户越多，传输越快。共享的理念和先进的技术使通过“海盗湾”分发的版权文献达到了惊人的数量，给版权持有人造成巨大损失。

出版商们因此将“海盗湾”视为眼中钉、肉中刺，必欲除之而后快。2006 年 5 月，瑞典警方以涉嫌窃密为由，突袭搜查“海盗湾”的数据中心，没收了许多服务器，这些服务器向约 100 个网站提供服务。不过，“海盗湾”的支持者非常强大，不到三天时间，“海盗湾”网站就重新开张了，而且由于媒体争相报道，“海盗湾”还增加了一大批新用户。此后针对“海盗湾”的诉讼一起又一起，“海盗湾”网站的运行也时断时续。一次，瑞典法院判决“海盗湾”关闭服务器，“海盗湾”就把位于斯德哥尔摩的服务器搬到荷兰。出版商又在荷兰起诉“海盗湾”，荷兰政府顶不住，也要求“海盗湾”搬走服务器，“海盗湾”不得不又把服务器搬回瑞典。这样来来回回折腾，“海盗湾”决心寻求避开各国法律约束的新途径。

二战期间，英国在为了对抗德军，将一座驳船凿沉，建成用于监视和预警来犯之敌的海上平台，平台面积 500 多平方米，比标准篮球场稍大一点。二战后这座平台就被废弃了，1967 年 9 月，英国人罗伊·贝茨一家搬了上去，宣布建立独立的“西兰公国”。尽管未获任何一个国家承认，“西兰公国”还是通过颁

布宪法、发行货币、设置国家机构等方式宣示主权。1968 年英国法庭判定，西兰平台位于公海，英国政府对其无管辖权，“西兰公国”借此宣称主权得到了承认。2007 年，“西兰公国”刊登出售广告，“海盗湾”旋即宣布欲出资购买，以避开任何国家版权法的约束。不过“西兰公国”最终没有接受“海盗湾”的收购请求，“海盗湾”独立建国梦就此搁浅。

“西兰公国”纪念“独立”50 周年

图片来源：“西兰公国”官方网站 http://www.sealandgov.org

“海盗湾”是盗版界的一面旗帜，在欧洲很多国家拥有大量支持者。为了获得政治实力和政策影响力，“海盗湾”的支持者成立了以反版权保护为核心理念的海盗党，2009 年，瑞典海盗党成为第三大党，并在欧洲议会选举中赢得了一个欧洲议会席位。“海盗湾”还计划以太空为基地建立自由王国，方法是发射一颗可搭载比特流服务器的地球轨道卫星。2010 年 10 月，“海盗湾”宣布将发射一颗卫星，将网站服务器运行在地球同步轨道上。为此，“海盗湾”聘请了专业技术人员，研究建立地球低轨服务器站点群的技术。