江苏省科协科普创新项目资助
中国网络空间安全协会竞评演练工作委员会指导

漫话 You Can! 信息安全

INFORMATION SECURITY

编著 袁志坚 王金双
缪嘉嘉 陈 融
绘图 徐小阿徐

江苏凤凰科学技术出版社 | 全国百佳出版单位

江苏省科协科普创新项目
中国网络空间安全协会竞评演练工作委员会指导

漫话 You Can! 信息安全

INFORMATION SECURITY

编著　袁志坚　王金双
缪嘉嘉　陈　融

绘图　徐小阿徐

江苏凤凰科学技术出版社 | 全国百佳出版单位

图书在版编目（CIP）数据

漫话信息安全 / 袁志坚等编著. -- 南京: 江苏凤凰科学技术出版社, 2016.1
ISBN 978-7-5537-5853-4

Ⅰ. ①漫… Ⅱ. ①袁… Ⅲ. ①信息安全－安全技术－普及读物 Ⅳ. ①TP309-49

中国版本图书馆CIP数据核字(2016)第000809号

漫话信息安全

编　　著　袁志坚　王金双　缪嘉嘉　陈　融
策划编辑　左晓红
责任编辑　陈　涛　朱　昊
责任校对　郝慧华
责任监制　曹叶平　周雅婷

出版发行　凤凰出版传媒股份有限公司
　　江苏凤凰科学技术出版社
出版社地址　南京市湖南路1号A楼，邮编：210009
出版社网址　http://www.pspress.cn
经　　销　凤凰出版传媒股份有限公司
印　　刷　江苏凤凰扬州鑫华印刷有限公司

开　　本　889mm × 1194mm　1/16
印　　张　6.25
字　　数　85000
版　　次　2016年1月第1版
印　　次　2016年1月第1次印刷

标准书号　ISBN 978-7-5537-5853-4
定　　价　32.80元

序言

让信息安全更加普及

早就答应出版社要编写一本信息安全的科普读物，平时也做了很多信息安全科普的演讲，但因为长时间的忙忙碌碌，一直没能兑现这一承诺。当然，如何能够把信息安全知识科普化，对我来说也是一种挑战。《漫话信息安全》一书的出现，让我眼前一亮：这就是我所期盼的信息安全科普读物。

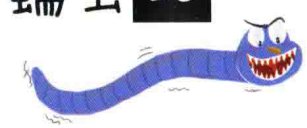
首先，《漫话信息安全》的推出非常重要。随着网络与信息技术的飞速发展，互联网已经深入到普通老百姓的日常生活，低龄化趋势明显，第三方数据显示我国青少年网民超过一亿。然而，信息安全作为信息技术的一种伴生性技术，仅了解信息技术，不了解信息安全技术，无疑像独轮车，难以平衡。显然，想要最大限度地让青少年享用互联网带来的红利，还需要家长、学校和社会给予更多引导，帮助他们适度用网、健康用网、安全用网。

其次，《漫话信息安全》非常吻合非专业人员的视角。普及信息安全，就是要让没有信息安全背景、甚至没有信息技术背景的人了解信息安全基本常识。因此，宣传信息安全知识就需要规避复杂的技术细节，不要让高深的数学方法把密码知识给封闭起来；不要让网络技术、操作系统、数据库等相关背景知识将非专业人士拒于网络安全概念之门外；不要让复杂的网络攻防技术细节让热血少年望而却步。《漫话信息安全》的出现，将会让缺少相关背景的读者如获至宝，它将那些拗口的名词、概念、定义、原理、事件等用通俗诙谐的话语重新组织，娓娓道来；通过漫话的形式，将难以直观理解的概念、原理用一幅幅漫画犀利剖析，使人有种豁然开朗的感觉。

最后，《漫话信息安全》开拓了青少年信息安全教育的新形态。中央网信办主任鲁炜强调，信息安全要从娃娃抓起。专业教育科普化、低龄化，已经成为一种教育时尚潮流，例如计算机领域的少儿编程、少儿机器人等。在网络与信息化程度高度发达的今天，信息安全方面的常识，应该像交通安全、饮食卫生、人身安全保护一样，成为青少年教育的必需。信息安全教育者理应放下自己的身段，站在娃娃的角度，满足他们求知的渴望。

我相信，《漫话信息安全》开了个好头，也希望更多的普及性科普作品问世。

中国工程院院士：方滨兴



江苏省科协科普创新项目
中国网络空间安全协会竞评演练工作委员会指导

漫话 You Can! 信息安全

INFORMATION SECURITY

编著　袁志坚　王金双
缪嘉嘉　陈　融

绘图　徐小阿徐

江苏凤凰科学技术出版社 | 全国百佳出版单位

维基解密

维基解密事件

2010年7月26日，一个叫“维基解密”的网站在《纽约时报》、《卫报》和《镜报》等传统媒体的配合下，在网上公开了数十万份的驻阿富汗美军秘密文件，引起轩然大波，这就是维基解密事件。

这一事件被认为是美国1971年“五角大楼文件泄密案”的升级版。

Wikileaks：成立于2006年12月的维基解密，是一个国际性非营利媒体组织，专门公开来自匿名来源和网络泄露的文件，目前约有志愿者1200人。

网站已公布的资料包括：有关阿富汗战争的文件、有关伊拉克战争的文件、美国外交部相关文件等。

维基解密的宗旨

维基解密官方说法，维基解密网站试图成为秘密文件的匿名集散地，这些文件的来源无法追查，也不受审查，最终揭露那些存在暴政的政府和公司不道德的行为。维基解密坚信，只有增加政府活动的透明度，才能减少腐败，建设强大、民主的国家与政府。而这就需要监督，监督就需要公开的信息。在历史上，获取信息的代价是昂贵的，现在随着技术的发展，获取信息的成本不断降低，加密技术也使得传递信息的风险降低。

NO MAILBOX

NO ADDRESS

神秘的维基解密

NO TELEPHONE

维基解密虽然致力于揭开秘密，但它自己却深藏不露：网站没有公开办公地址、电话号码和办公邮箱，外界甚至不知道它的总部在哪。网站没有公布主要运营者的姓名，更不知雇员有哪些人。

朱利安·阿桑奇
Julian Paul Assange

ANONYMOUS

维基解密没有总部或传统的基础设施，该网站依靠服务器和数十个国家的支持者做了很多事情。上传材料的人也都是匿名，因此相对而言很少受到审查者、律师或地方政府的压力，也不受传统的新闻伦理以及平衡报道原则的限制。

苹果iCloud泄密

事件缘由

包括珍妮佛·劳伦斯、维多利亚·
嘉斯蒂、埃米莉·布朗宁、凯特·波茨沃斯、
珍妮·麦卡锡和凯特·阿普顿在内的多名好莱坞女明星
不雅照片外泄，爆料者并未一次性放出所有照片，
而是分批次逐步披露，
一波又一波的不雅照片推动这次事件
持续保持高热度和高关注度。

Let me tell you why

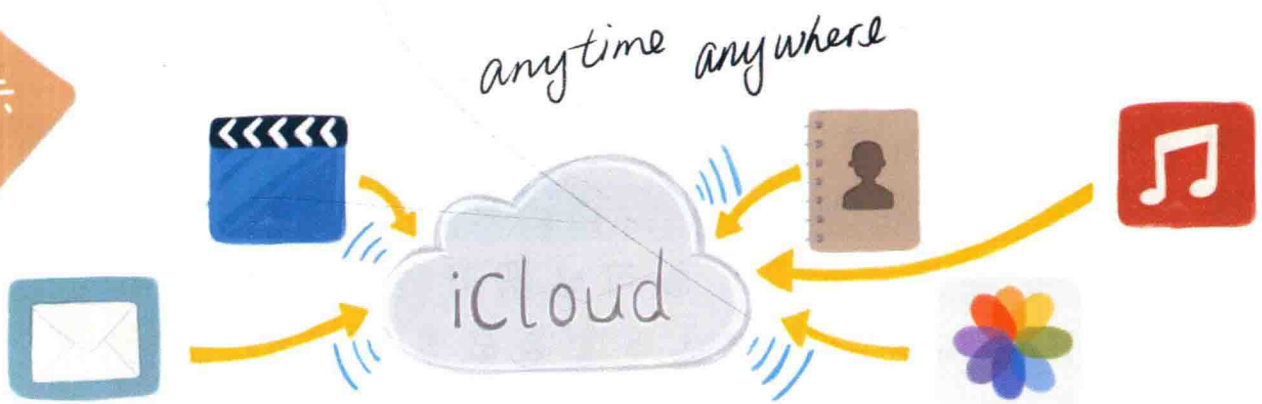
以往的不雅照片泄露，源头通常是个人电脑的使用不当。而这次的不雅照片泄露，源头是存储照片的苹果云存储服务iCloud。在人们的印象中，云存储服务提供商通常是大公司，非常值得信赖，尤其是非常注重安全与隐私的苹果公司。苹果认为泄密不是他们的责任，辩解道："我们发现某些名人账号遭到了针对用户名、密码和安全问题的定向攻击，这在网上已变得非常普遍。如果用户能够设置更复杂密码、定期更改密码以及注意异常登录提醒，可能减少这种事情发生"。

苹果公司的安全策略存在漏洞，黑客可以使用苹果公司所提供的FindMyiPhone的API，暴力破解iCloud账号/密码。

如何弥补呢？

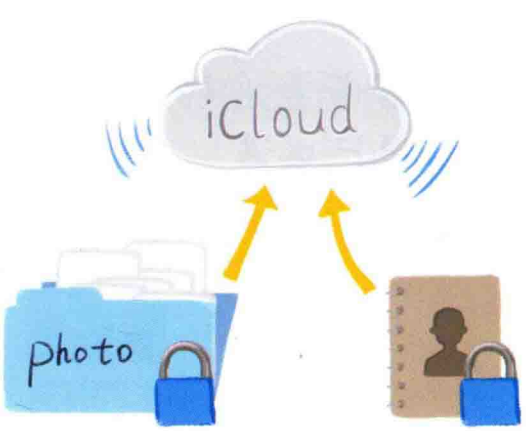
苹果可以限制账户每天的登录次数，也可以在“找回密码”方式上，通过手机进行二次验证。

启示



云服务作为新生事物，大大方便人们的日常使用。云服务最理想的情景是，不论何时何地，只要能够连接上互联网，每个人都可以享受便捷的云服务：上传/下载照片、备份通讯录、看电影、听音乐、协作编辑文档，就像我们享受电力、自来水提供的便利一样。

但是，使用云服务意味着数据安全的主动权交给了云服务提供商。用户与云服务提供商之间虽然签有隐私协议，但通常无人为此负责，因此，使用云服务的时候，用户还是需要多考虑一些安全问题，例如，预先对照片、通讯录进行加密，再上传到云端。

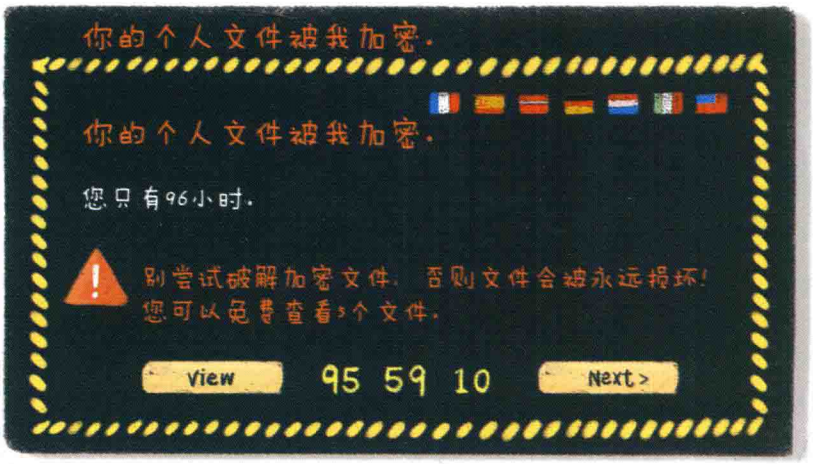


比特币敲诈者

事件由来

CTB-Locker

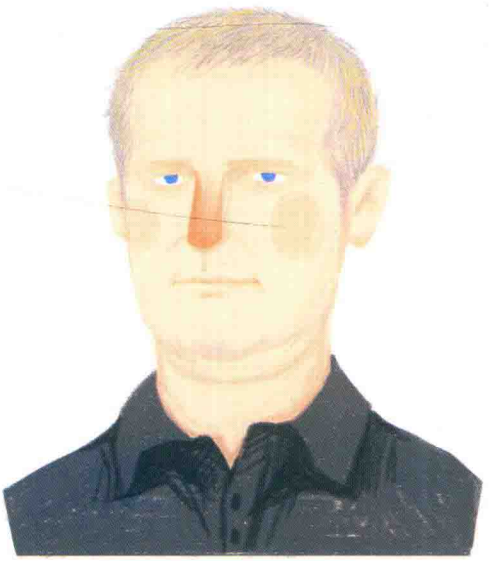
×8 =10000 RMB



2015年初，网络上流行一种新型病毒，中毒电脑里的文档、图片等重要资料被病毒加密。病毒同时提示受害者，只要在规定时间内（通常为96小时）交纳一定数额的比特币（通常为8比特币，约合1万人民币）作为赎金，就可以解开这些资料，否则这些资料都无法打开。病毒通常会让受害者免费解开5个文档，表明病毒可以解锁资料。这种病毒就是比特币敲诈者CTB-Locker。

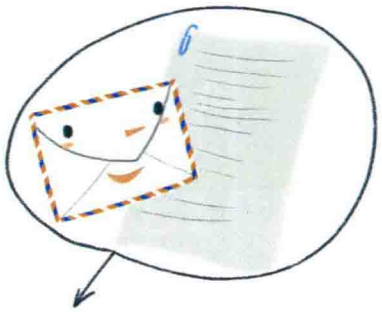
作者

病毒作者波格契夫来自俄罗斯，擅长编写僵尸病毒，美国FBI悬赏300万美元缉拿此人，在十大被通缉黑客中排名第二。



波格契夫

病毒特点



比特币敲诈者主要通过邮件附件传播，受害者大多是具有较好经济能力的高端人士，敲诈的赎金较高。同时这种病毒具有隐蔽性强、技术手段高明、危害高等特点。

为什么用比特币？

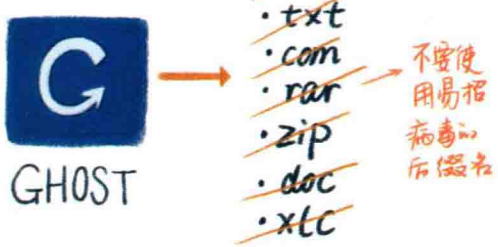
比特币并不是法定货币，但是具有一定的流通性和认可度，而且比特币交易完全匿名，不能通过账号追查到敲诈者的具体开户信息。另外比特币交易在随机匿名并且加密传输的网络中进行，这些都使得敲诈者可以轻易逃脱法律的制裁。

如何应对呢？

该病毒可以被杀毒软件查杀，但是还没有找到破解病毒加密的方法，因此一旦中毒，除了支付赎金，别无他法。防患于未然尤为重要：

1. 谨慎对待邮件中的附件，不要轻易打开附件，如果附件是压缩包，需查看压缩包的内容再决定是否打开。

2. 使用加密软件定期备份系统中的重要数据，并将备份数据包的后缀名改为自定义的后缀名。



熊猫烧香

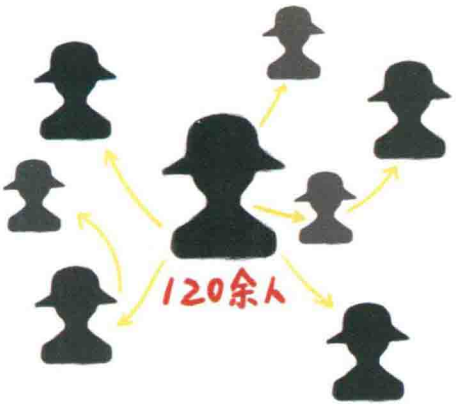
2007

2007年初，因特网肆虐着一种蠕虫病毒，受感染电脑的可执行文件图标均变为憨态可掬烧香膜拜的熊猫，还会出现蓝屏、频繁重启以及文件被破坏等现象，电脑几乎无法使用。这种病毒就是显赫一时的熊猫烧香病毒。

病毒作者李俊，
后来被捕并被判刑四年。

李俊当时24岁，中专学历，沉默木讷。从水泥厂辞职出来，只身一人前往武汉打工，卖电脑，做网吧管理员，后来编写“熊猫烧香”病毒。

李俊以3000元的单价，将“熊猫烧香”病毒卖给120余人。



熊猫病毒买家购买病毒后大肆传播，被“熊猫烧香”病毒控制的电脑数以百万计，受控电脑访问按流量付费的网站，一年下来网站累计可获利上千万元，而造成的损失估计高达上亿元。

被捕后，
李俊曾如此描述走进黑客世界的感觉

在这个群里，只要你是高手，其他人都会佩服你，追捧你，崇拜你。我非常开心……我发现自己越来越离不开网络了，那里有我的自尊，有我的能力被认同的成就感……

2009

2009年底，李俊因在狱中帮助狱警做电脑方面的工作提前出狱。在多家网络安全公司求职碰壁后，李俊选择自己创业。

2013

2013年底，李俊再次成为新闻人物，因伙同他人开设网络赌场，被浙江丽水莲都区人民法院，以开设赌场罪判处有期徒刑三年。曾发誓“浪子回头”的他，最终却还是违背了自己的誓言，重入歧途。他的人生就像是中了某种病毒，兜兜转转，循环往复。

心脏出血

Heartbleed

事件由来

2014年4月8日，谷歌安全团队和芬兰网络安全公司Codenomicon宣布，网络安全协议SSL的软件包OpenSSL存在心脏出血漏洞。https协议基于SSL协议实现，而https网站应用范围极其广泛，因此心脏出血漏洞影响巨大，业界为之震动。

Influence

影响

所有https网站都受心脏出血漏洞影响。据不完全统计，Alexa排名前百万的网站有近40%受影响，其中中国至少有几万。腾讯的微信/QQ/邮箱、阿里巴巴的支付宝/淘宝，知乎、京东/苏宁/盛大、12306、360等……从电商到即时通讯，从社交媒体到安全公司，知名网站几乎无一幸免。

Remedial measures

补救措施

由于心脏出血漏洞非常致命，安全公司在漏洞发现的第一时间发布了修改漏洞的补丁程序.网站除了更新补丁程序外，还需要更新已失效的X.509安全证书，更换泄露的密钥。