<<黑客的代码>>

图书基本信息

书名：<<黑客的代码>>

13位ISBN编号：9787511323910

10位ISBN编号：751132391X

出版时间：2012-7

出版时间：辽宁教育出版社

作者：马克·拉希诺维奇

页数：264

字数：260000

译者：钱峰

<<黑客的代码>>

内容概要

一组名为“超级瘾君子”的神秘代码何以让全球陷入恐慌。

这部由国际知名的网络安全专家写成的作品，向我们展现了一幅令人恐惧的未来画面，一个如今无法想象、却完全忠实于科技的世界。
无论是国家安全还是个人隐私在如今庞大的网络系统中都存在安全隐患。

阿拉伯人为了报复以美国为首的西方国家，决定雇用黑客入侵这些国家的计算机，于是一种名为“超级瘾君子”的病毒横扫计算机世界……一架客机的操控装置在大西洋上空失灵；一艘油轮的导航系统突然失控，油轮在日本搁浅；各地医院给病人开出错误用药剂量导致病人死亡，医院被迫放弃使用计算机数据库……这些计算机故障看似是偶然事件，彼此互不关联，实则蛰伏着神秘黑客的惊世阴谋。

作者简介

马克·拉希诺维奇是微软公司的技术院士——全公司最重要的技术职位，也是享誉世界的Windows内核技术专家，Sysinternals的创建者之一。
他还开发了很多用于Windows管理和诊断的工具。
马克于1989年获得卡内基梅隆大学的计算机工程学士学位，次年获得伦斯勒理工学院硕士学位。

1994年又得到卡内基梅隆大学授予的博士学位。

章节摘录

当他把光盘放入服务器的光驱时，他首先想到的是，不管这里发生了什么，都是由已有的病毒成千上万的新变种之一引发的，这些病毒经常出现，每月多达50种。
他希望这是已有病毒的新品种，希望这是某个学生黑客放出来为了获得一些吹嘘的资本。
苏可能也那么想过。
即使是那样，可能也是一项困难的工作，但他还是可以应付。
那样的话，也许可以完全，或者近乎完全地恢复数据，因为公司需要的数据还会在服务器的某个地方。
但是杰夫自己的操作系统运行之后，他注意到的第一件事是他不能发现硬盘上的任何数据。
仿佛硬盘从来都没有安装过操作系统，甚至标准C盘驱动程序图标也消失了。
他从没见过这种情况，顿时感到脊骨发凉。
怎么可能呢？
他寻思着。
他意识到这将不是惯常问题，既兴奋又担心。
苏在他身旁的计算机前坐下，她皱着眉说：“叫我‘万人厌’小姐吧。
他们的反应好像是我放的病毒。
”她看着他的屏幕，“有什么收获吗？
”　　杰夫告诉她目前为止他所做的和所想的。
“给我一张你那可爱的启动CD。
”　　杰夫笑了，看起来像个12岁的男孩。
“除非你杀了我。
”这CD是他上千个小时辛苦工作的结晶，在很多情况下，正是它促成了他的成功。
他不止一次地开玩笑说打算把这张CD带进棺材。
“你准备做什么？
”他问。
苏撅起嘴：“我要白费劲了，可能分析防火墙和代理服务器日志，如果这对你有用的话。
”杰夫点点头。
那一块需要着手，如果她做了，可以节省时间。
“也许我会撞上什么有用的东西。
这根本不是我的工作范围。
”　　“可能你会走运。
”杰夫鼓励她说。
苏开始工作后，他运行了一个抢救工具，这个工具可以进行一些猜测，并忽略那些看起来有些像错误的东西。
有了这个帮手他成功的可能性就更大了，它可以使他看到之前看不到的文件和文件夹。
现在可以扫描硬盘剩余数据了，杰夫搜索着包含了系统核心配置的文件。
可他发现的却是原始操作系统的零碎残片以及部分程序数据的临时拷贝。
他有些失望，不过还是可以用其数据库重建部分文件系统和注册信息。
数据库存储了设置和针对计算机操作系统的不同选项。
至少这是个开始，他想。
下一步，他浏览了损坏了的注册条目。
这有点像扫描电视导航看看在播放什么节目，而不是看上一整个晚上的节目。
他发现部分数据被覆盖了，这一标准意味着数据被破坏。
已有数据之上又覆盖了随机符号，因此原始数据很难恢复，有时候甚至不可能恢复。
但是奇怪的是只有一部分原始数据被覆盖了。
杰夫心想，如果那就是病毒的意图，那它还没有完成。

有几种可能的解释。
最明显的是破坏性病毒的存在，破坏性病毒由于其本身的一个故障，覆盖程序中止了。
这种病毒本可能引发导致操作系统崩溃的行为，而操作系统的崩溃中止了病毒，覆盖程序就半途失败了。
如果这就是全部情况的话，还不是非常复杂。
真正有效的病毒永远也不会破坏驱动程序和操作系统，这两者可是它的寄主。
那有点像疾病在没传染其他人之前就把主人杀死了。
最有效的病毒是那些隐藏在计算机中的，而操作者一点儿也不知道。
在操作系统被摧毁之前，这样的病毒应该会设法复制传播以免于被发现，虽然传播速度缓慢。
但目前这种情况，病毒的某个部分攻击了系统，实际上就是自杀了。
现在杰夫扫描了崩溃的注册文件设置。
恶意软件常会创建条目，这样，每次打开计算机或用户登录时操作系统就会将它们激活。
他检查了每个条目，甚至是那些看起来并不可疑的条目。
当他定位了某个程序的出处或没有发现的密码时，他会找到密码文件，更为仔细地进行检查，查看该文件是否提供了与其关联的产品和撰写该文件的公司，因为恶意软件往往缺少类似信息。
然后他进行了网络搜索，寻找文件目的的信息，查看之前有没有人称其为恶意软件。
这项工作乏味而耗时，但它是处理此类问题的核心部分。
疲惫感再次袭来，起初一闪而过的兴奋退去了。
不过疲劳工作稀松平常。
在此类情况中，时间就是一切。
然而目前为止还没有任何进展。
两小时之后，杰夫发现一个设备驱动程序的出处有些可疑，总算有了一点突破。
设备驱动程序是这样一种程序——它允许其他程序（如打印机）与一点硬盘空间相互作用，恶意软件写手青睐这种程序，因为可以利用它们编写不被标准安全保护软件发现的间谍软件、病毒、恶意广告软件。
大部分家用个人计算机都带有这种类型的恶意软件，机主甚至都不知道。
所有设备驱动程序都有包含磁盘文件路径的信息。
磁盘文件包含了驱动程序密码，因此杰夫可以毫不费力地定位可疑驱动映像。
有一个文件，ipsecnat.sys，名字似乎和合法、标准的驱动程序很相似，他没有认出来。
当他检查时，这个文件的版本信息显示它属于微软，但是在网上搜索发现驱动程序并没有这一名字的文件。
我的队伍又多了一个成员，他想着。
杰夫顿时精神抖擞，将这个驱动程序载入代码分析器，这个分析器可以把计算机执行的指令转化成人类可读的版本。
在这一水平分析恶意软件是他工作的一大部分，因此他可以在大脑中像计算机一样过一遍指令。
这样他可以理解所有的意图。
他读着：.text：00000000007B35D8xor[rcx+30h]，rdx .text：00000000007B35DCxor[rcx+38h]，rdx .text：00000000007B35E0xor[rcx+40h]，rdx .text：00000000007B35E4xor[rcx+48h]，rdx .text：00000000007B35E8xor[rcx]，edx .text：00000000007B35EAmovrax，rdx .text：00000000007B35EDmovrdx，rcx .text：00000000007B35F0movecx，[rdx+4Ch] .text：00000000007B35F3loc_7B35F3 .text：00000000007B35F3xor[rdx+rcx*8+48h]，rax .text：00000000007B35F8rorrax，cl .text：00000000007B35FBlooploc_7B35F3 .text：00000000007B35FDmoveax，[rdx+190h] .text：00000000007B3603addrax，rdx .text：00000000007B3606jmprax 读完之后，他十分警觉。
很明显代码被加密了。
病毒经常将自己加密，使得病毒扫描者花费大量时间解开核心代码，甚至不可能解开。
发出之后，恶意软件将其本身解码，进入存储器，这一过程根据采用的加密方案的水平和复杂程度需

要几秒钟。
那也是为什么计算机启动缓慢常常是感染病毒的一个迹象。
　　接下来的三个小时过得飞快，杰夫试图将黑客使用的加密算法和那些恶意软件写手常常使用的相比照。
最终，他确定这是新品种。
这部分工作对他就像一个谜，他与黑客较量创造力和意志力。
它本身和他玩过的最难的计算机游戏差异并不是太大，只不过现在具有真正的危险。
杰夫知道这一点，因此兴奋不起来，不过在继续之前他禁不住在精神上鼓励自己。
　　作为预防措施，他设了一台本质上是“虚拟的”计算机，他可以用它检查运行中的病毒，但速度要慢得多。
虚拟计算机运作起来就像实体计算机，而且对用户来说，它看起来像实体计算机的屏幕呈现在台式机的窗口中。
但是这台虚拟计算机使杰夫能够很好地控制过程，他可以控制恶意软件的执行，按照他的需要开始和停止运行恶意软件。
他希望能够通过这种方法解开代码。
　　然后，他将代码作为驱动程序未加密拷贝到光盘上。
他完全沉浸其中，忘记了白天黑夜，甚至忘记了苏的存在，她从他的世界消失了，虽然她还坐在他旁边。
他既不渴也不饿，完全不觉得身体有什么不舒服。
　　他总感觉他天生就是做这种工作的，在这样的工作中，他可以忘记其他一切。
对他而言，解决一个计算机问题就像解决一道谜题，他酷爱那些游戏。
而且他讨厌失败。
真实世界可能混乱、充满暴力，他常常感觉自己无法控制。
但从事这类工作，他可以了解计算机，甚至攻击计算机的病毒。
在这里，成功得到了明确的定义：他完工之时，计算机要么开始工作；要么不工作。
　　现在，面前的屏幕就是他唯一的世界。
　　……

媒体关注与评论

马克于2006年加盟微软，参与推进更新Windows，他的最新作品引人入胜，让人们对网络恐怖主义威胁有了更深刻的认识。

——比尔·盖茨　　网络恐怖主义。

习惯这个词，理解这个词吧，在不远的未来，你会在报纸上看到、新闻中听到更多有关这个词的报道。

马克·拉希诺维奇是网络安全专家，他把自己丰富的知识转化成一部令人惊恐又相当可信的小说。

《黑客的代码》不是科幻小说，而是科学事实，它清楚地提醒人们末日的来临。

所有美国人，以及那些与我们的安全和生存息息相关的人都必须读一读这部小说。

——美国著名惊悚小说作家：尼尔森·迪米勒　　马克小说中的一系列危险情节正是我们当今看到的许多事实的写照。

——白宫网络安全协调官：霍华德·施密特　　《黑客的代码》是一部紧跟时代步伐，情节紧凑，步步紧逼的惊悚小说，用一种令人惊恐却使人信服的方式重现“9·11”。

作为此领域的专家，马克·拉希诺维奇以技术上的权威和极大的热情描写网络恐怖主义。

我着实被吸引住了。

”　　——《扼杀者》作者：威廉·兰迪　　“这是一部紧跟时事，充满阴谋、背叛、暴力的优秀惊悚小说。

”　　——《科克斯书评》　　拉希诺维奇的首部惊悚小说值得一读，特别是对于那些阴谋论者，他们会相当喜欢。

”　　——《图书馆杂志》

<<黑客的代码>>

编辑推荐

亲，如果你想保护好自己的隐私，一定要读读《黑客的代码》！
《黑客的代码》是微软技术高管马克·拉希诺维奇，根据自己在从事系统开发过程中遇到的一些真实事件编撰而成，意图揭示隐藏在地球背面的黑客世界，内容超出想象，却又完全忠于科技。
获得过比尔·盖茨及白宫网络安全协调官：霍华德·施密特的大力推荐！

版权说明