DONG'S VIEW
ON SECURITY

大东话安全之网络病毒篇

翟立东◎主　　编
中国网络空间安全协会 中国科学院计算技术研究所◎指导单位

幽默中解析网络病毒，笑谈间指引网安之路

网安新时代即将到来

DONG'S VIEW
ON SECURITY

当万物互联遇上安全问题，我们摒弃晦涩的术语
只在乎 ——— 如何保护连接的万物和你
怀着一颗好奇之心，用着最简单的语言
来，听我们大话安全

机械工业出版社
CHINA MACHINE PRESS

大东话安全之网络病毒篇

主　编　翟立东

副主编　张旅阳　郑　昕

参　编　陈　曦　都丽丽　李维森　潘远聪

吴静慧　尹玲鑫　张智高　赵　洋

机械工业出版社

本书将近年来计算机病毒的发现过程进行梳理，以浅显轻松的方式展现出来，使读者对其有初步了解，从而引起读者对信息安全的兴趣。书中涵盖了近年来 54 个病毒事件的始末，并对每个病毒的原理、危害和预防进行分析，语言通俗易懂，轻松活泼，并结合当下热点，借鉴漫威漫画的架构，大大提高了读者的阅读兴趣。

本书涉及的专业知识不需要很深的计算机知识作为前提，不管你是谁，无论你来自哪里，无论你的背景或教育如何，都能理解、掌握和使用书中论述的观点。

图书在版编目（CIP）数据

大东话安全．网络病毒篇 / 翟立东主编．—北京：机械工业出版社，2018.6
ISBN 978-7-111-60362-7

Ⅰ.①大… Ⅱ.①翟… Ⅲ.①计算机网络—网络安全 ②计算机病毒—防治 Ⅳ.①TP393.08 ②TP309.5

中国版本图书馆 CIP 数据核字（2018）第 146486 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策划编辑：汤 枫 责任编辑：汤 枫
责任校对：张艳霞 责任印制：孙 炜

北京中兴印刷有限公司印刷

2018 年 7 月第 1 版第 1 次印刷
184mm×260mm • 15.25 印张 • 264 千字
0001－3000 册
标准书号：ISBN 978-7-111-60362-7
定价：49.00 元

服务咨询热线：（010）88361066 机 工 官 网：www.cmpbook.com
读者购书热线：（010）68326294 机 工 官 博：weibo.com/cmp1952
（010）88379203 教育服务网：www.cmpedu.com
封面无防伪标均为盗版 金 书 网：www.golden-book.com

前　言

网络空间作为继陆、海、空、天之后的第五维空间，对我国人民生活产生了日益深远的影响。当前，网络空间安全正在国际格局中扮演着越来越重要的角色，日渐成为国际舞台博弈和角力的重要议题和国家安全的战略高地。习总书记曾经指出：“没有网络安全就没有国家安全，没有信息化就没有现代化”。网络安全的科学普及工作自然也被社会各界视为维护国家网络安全和建设网络强国的重要一环。

在复杂的社会信息环境中，网络空间安全的科学普及工作形势显得尤为严峻。一个人的力量总是有限的，能够整合行业资源，让业内学者、政府和企业工作人员共同参与，才能获得真正优秀的网络空间安全科普作品。本书按照 54 个病毒线索构成的一整副扑克牌形式展开，包括大王 APT、小王商业军火、13 个黑桃 APT、13 个红桃移动威胁、13 个梅花木马、13 个方片蠕虫，总计 54 张扑克牌，54 个病毒。

在此感谢中国网络空间协会秘书长李欲晓、褚诚缘的支持，感谢原贵州省政协副主席谢晓尧、贵州省网信办常务副主任刘翀、贵州师范大学大数据与计算机科学学院苏明院长和阮方鸣老师的指导，感谢中科院计算所程学旗、王元卓、刘悦、沈哲等老师和同事的悉心关怀，才有本书的问世。

由于编者水平有限，书中难免有疏漏之处，恳请读者提出批评与指正，以便进一步修订与完善。

编　者

目　录

梅 花 篇

方 片 篇

大东话安全 Plus

开 篇 词

浪淘沙　网安风云

秋光照幽索，辕衣婆娑。单于观兵白登道，都护传檄冠军侧，烽烟朔漠。流沙逐瀚海，横刀关河。万马夺旗成一快，为报吮疽荡熊魔，血染长辙。

王　篇

大东话安全之“魔”——APT

一、开场小剧场

马云：我就是打着望远镜也找不到竞争对手了。

东哥：那是因为对手骑在了你的脖子上。

小白：东哥说得没错！

二、病毒通缉令

东哥和小白说的是什么？其实他们说的是这张牌的内容——

小白：这牌上炸毛的骷髅比楼还大，难道要吞了它？这不科学！

大东：这是 APT（Advanced Persistent Threat，高级持续性威胁），它的威力岂止是吞噬一栋楼那么简单。

小白：APT 是什么？

大东：APT 是当前企业和组织面临的最严峻的安全威胁，在 APT 攻击中，攻击者投入大量人力、财力和时间，综合运用社会工程学以及 0day 漏洞，进行目的明确的针对性攻击，从而造成严重的损失。在 APT 攻击中，恶意代码，尤其是利用漏洞的恶意代码，扮演了极其重要的角色。

小白：没听懂。

大东：别急，下面慢慢说。

三、大话始末

大东：要说 APT 是何许毒，还得从 2010 年震惊寰宇的“震网”事件说起。

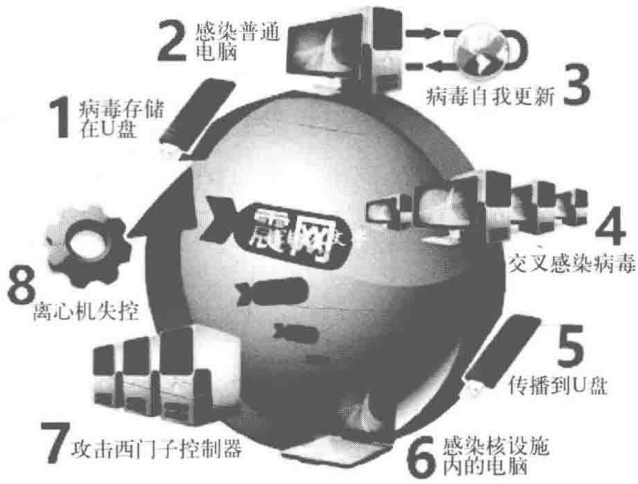
2006 年，伊朗在纳坦兹核工厂安装了大批离心机，进行浓缩铀的生产。但令伊朗大跌眼镜的是，核工厂的运行极不稳定，离心机的故障率居高不下，核武器所急需的浓缩铀迟迟生产不出来。技术人员反复检查，却找不出任何故障原因，离心机出厂时明明是质量合格，一旦投入运行，却马上就会磨损破坏。伊朗人实在弄不清出了什么问题。

小白：怎么发现这就是 APT?

大东：当伊朗核工厂在跌跌撞撞中挣扎的同时，信息安全界发现了另一件看似不相关的事件。2010 年 6 月，白俄罗斯的一家安全公司 VirusBlokAda 受邀为一些伊朗客户检查系统，调查他们计算机的死机和重启问题。技术人员在客户计算机中发现了一种新的蠕虫病毒。根据病毒代码中出现的特征字“stux”，新病毒被命名为“震网病毒（stuxnet）”，并加入公共病毒库中，公布给业界人士研究。

起初，研究人员以为，这不过是千万种流行病毒中的一种，并不以为意。但进一步的深入研究却让他们瞠口结舌：“震网”病毒的复杂度远远出乎人们的意料，它是当时所发现的最精妙、最复杂的病毒，没有之一，而且病毒中居然还含有两个针对西门子工控软件漏洞的攻击，这种针对工业控制系统的蠕虫病毒在当时是

绝无仅有的。随即，“震网”病毒引起了信息安全界的极大兴趣，随着更多专家投入到对它的分析，它的面纱被渐渐揭开——它跟以往流行的病毒完全不一样，这是世界上第一例针对工控系统的病毒，更精确地说，它是为伊朗纳坦兹核工厂量身定做的病毒武器。



“震网”病毒传播过程

小白：这个震网病毒是怎么传播的？

大东：经事后调查，“震网”病毒是经由工程师的 U 盘，从普通计算机转移到核设施内部的计算机，而且“震网”病毒的攻击方式非常狡猾，它渗透进入核工厂后并没有一举摧毁整个工厂，而是悄悄地潜伏下来，每隔一个月才攻击一次。攻击期间，它会首先修改西门子工控系统的数据，让离心机看上去运转正常。但背地里，它却大幅提高离心机的转速，迫使其在临界速度以上运转，从而迅速毁坏一台离心机。“震网”病毒强大的隐蔽性，使得伊朗人更换了数批工程师，却一直找不到问题原因，白白损失资金和时间。

小白：APT 好厉害！

大东：这就是典型的 APT 特征——幕后操纵者强大的掌控力，目标准确，潜伏时间长，隐蔽性高。APT 的攻击与否完全取决于目标对象是否有足够的攻击价值。

小白：明天先换个新 U 盘去！

四、小白内心说

小白：如今的社会中，计算机服务于各行各业，尤其是关系到国计民生的银行、电力能

源、军事等行业部门，这些部门的数据万一受到攻击，后果不堪设想！

大东：确实，能源、通信、政府等关键部门的数据对我们国家建设来讲，其重要性不言而喻。然而，总有黑客想窃取数据，为了能获取重要数据，不惜潜伏数月甚至数年，持续不断地进行网络攻击和数据窃取。

小白：真可谓是艰苦卓绝，孜孜不倦！

大东：如今具有潜伏性和持续性的高级持续性威胁已成为我国网络安全威胁的常态，重大的黑客攻击行为也常常隐藏在不间断的小打小闹中，攻击的目标依然集中在金融、工业和政府部门，攻击手段丰富多样，0day 漏洞、恶意代码、钓鱼水坑等各种攻击方式层出不穷，APT 已经影响到每一个人的生活。

五、话说漫威

小白：说了这么多，APT 到底是什么东西？

大东：漫威电影你看过没？

小白：呃。

大东：在漫威电影里，复仇女神死后化身成为七颗无限宝石，除了自我宝石，其他六颗宝石身上都隐藏着巨大的能量，拥有宝石者则拥有了宝石的能量。APT 就像是最强大的意念宝石，能够控制他人心智，黑化好人，为己所用。

APT 的提出，使网络战争成为一种新型的战争方式。它更持久，更隐蔽，却具有更强大的破坏效果。网络战争新时代的大门已经开启，下一次战争会怎么打？没人能预料。

大东话安全之“道”——商业军火

一、开场小剧场

《庄子·胠箧》：彼窃钩者诛，窃国者为诸侯；诸侯之门而仁义存焉。

东哥：偷窃带钩的杀头，偷窃国家的做诸侯。简直无仁无义！

小白：无情无义无理取闹……

二、病毒通缉令

小白：酷！骷髅大兵既视感！这张牌太帅了！

大东：帅什么，又是火箭筒，又是子弹手雷，都是武器，一看就不是什么善茬。

小白：大东东，你不懂年轻人的审美！这是什么？

大东：这是商业军火，与以往的 APT 事件相比，其成本门槛不高，使得缺少雄厚资

金、没有精英黑客的国家和组织依托现有商业攻击平台提供的服务即可达到接近APT级攻击水准，今后将有更多的攻击者将现成的商业攻击平台作为军火使用。

小白：病毒小批发市场既视感！

三、大话始末

大东：前面所说的APT是针对能源、通信、政府这样的国家重要机构，而商业军火却是民间行为，技术门槛也相应低了很多。

小白：商业军火到底是什么？

大东：其实商业军火可以理解为一种低配版的APT，WannaCry（想哭）和Petya你知道吗？这种勒索病毒就是很典型的商业军火。

小白：当然不知道。

大东：WannaCry是一种“蠕虫式”的勒索病毒软件，大小只有3.3MB，不法分子利用此前披露的Windows SMB服务漏洞（对应微软漏洞公告：MS17-010）攻击手段，向终端用户进行渗透传播。

小白：这么大点的东西居然有这么大威力？

大东：这是由于它的传播机制导致的。该恶意软件会扫描计算机上的TCP 445端口（Server Message Block/SMB），以类似于蠕虫病毒的方式传播，当用户主机系统被入侵后，弹出勒索对话框，提示勒索目的并向用户索要比特币。而对于用户主机上的重要文件，如照片、图片、文档、压缩包、音频、视频、可执行程序等几乎所有类型的文件都被加密，加密文件的后缀名被统一修改为“.WNCRY”。

小白：真是怕什么来什么！

大东：目前，安全业界暂未能有效破除该勒索软件的恶意加密行为，用户主机一旦被勒索软件渗透，只能通过重装操作系统的方式来解除勒索行为，但用户的重要数据文件不能直接恢复。而此次爆发的WannaCry病毒很快又出现了变种，该变种传播速度可能会更快。

小白：但是真的有变种吗？

大东：当然有，不到两个月，乌克兰警方2017年6月28日透露，已接到近200通关于计算机被“勒索”的报警电话。乌克兰总理格罗伊斯曼表示，这轮病毒的攻击规模“前所未有”，但多数重要系统没有受到重创。俄媒援引网络安全专家分析指

出，此次情形与 2017 年 5 月 WannaCry 病毒在全球众多国家爆发的情况颇为相似，或为 WannaCry 病毒的新版本，但目前来看规模明显要小。

小白：这可真是一个坏消息！

大东：实施这波“勒索”的幕后黑手现仍不明，但据全球多家知名网络安全公司分析，乌克兰会计软件 MeDoc 可能被用于最初的感染源。乌克兰网络警察确认了这一消息，但这家乌克兰公司予以否认，恐怕很难找到幕后黑手了。

四、小白内心说

小白：东哥，我以前一直觉得，木马病毒最多就是删除文件，篡改数据，没想过还能当武器军火来玩。

大东：在震网病毒之前，人们更多认为计算机病毒破坏的是计算机本身，删除文件，篡改数据，损失的只是文件和数据。震网病毒曝光后，突然发现，计算机病毒居然也能用来做武器，去攻击其他国家的工业设施。臭名昭著的 Wannarcry 勒索病毒更是让很多人损失惨重，欲哭无泪。

小白：我觉得将来肯定会出现越来越多的网络军火！

大东：如今战争的层次已经不仅仅局限在海陆空等领域，网络空间成了大国较量的新战场。网络空间战争的武器已然不是传统的刀斧棍棒和长枪短炮，网络空间的安全攻击也不是普通盾牌装甲能抵御的。未来大国竞争的焦点或许会规避大规模杀伤性武器，转而开发更加隐蔽的网络空间武器。只是不管网络武器如何厉害，提高警惕才是解决之道。

五、话说漫威

小白：APT 是意念宝石，这个商业军火怎么说？

大东：时间宝石，它是至尊法师的神器，在电影《奇异博士》中被叫作“阿戈摩托之眼”。

这颗宝石能让使用者到达任何一个时间点，无论是久远的过去，还是遥远的未来，使用这力量可以观看或体验任何时代。如果使用者具备丰富的知识，则可以做更多的事情，甚至是操纵时间和因果。在香港街道大战的一幕中，为了扭转败局，奇异博士不得已开启“阿戈摩托之眼”，静止时空并扭转了时间的状态。他

利用时间宝石的能力，去和多玛姆谈条件，如果多玛姆不同意离开地球，那他就会永远深陷在时间里循环。

小白：厉害了！商业军火就像是这颗时间宝石吗？

大东：没错！商业军火就如同电影中的时间宝石，虽然现在还没有人能够轻松自如地操纵它，但是一旦出现势力强大的操作者，商业军火的危害将会遍及全球。因为与以往的 APT 事件相比，其成本门槛不高，使得一些缺少雄厚资金、没有精英黑客的国家和组织依托于现有商业攻击平台提供的服务即可达到接近 APT 级攻击水准，今后将有更多的攻击者将现成的商业攻击平台作为军火使用。

小白：一面是强大，一面是威胁！生存还是毁灭，这是个问题……

黑桃篇

大东话安全之“横”——毒菌行动

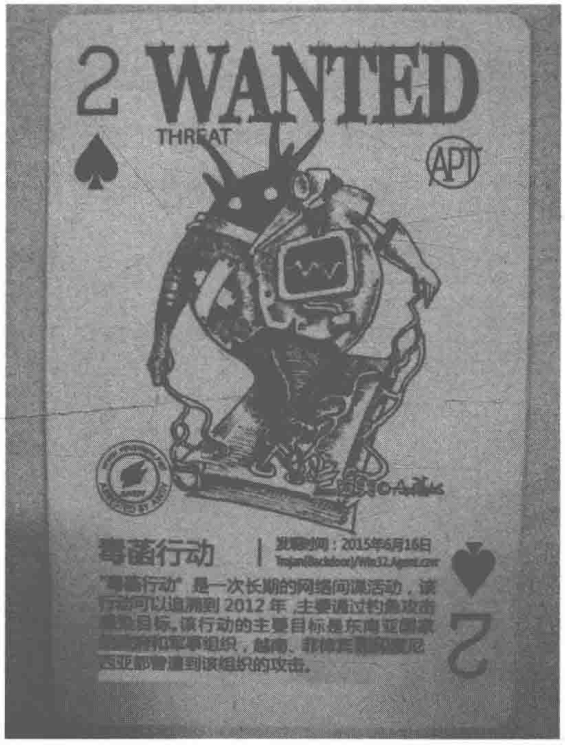
一、开场小剧场

新闻：手机支付势不可挡，现金支付正在过时！

大东：移动安全要提高，“无现金时代”还有多远？

小白：捡钱难！

二、病毒通缉令



小白：这是什么怪物？神偷奶爸究极进化？出门还骑着稿纸呢。