奇安信 新一代网络安全领军者

网络安全科普丛书

ADVANCED PERSISTENT THREAT

Cyberspace

奇安信威胁情报中心

/著/

透视APT

赛博空间的高级威胁

读网络安全科普书 看网络安全新鲜事

洞悉无处不在的威胁 掌握保护自己的武器

让网络更安全 让世界更美好

中国工信出版集团

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络安全科普丛书

ADVANCED PERSISTENT THREAT

—— Cyberspace ——

奇安信威胁情报中心

／著／

透视APT

赛博空间的高级威胁

電子工業出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 简 介

网络安全是一场无休止的攻防战。十几年前，网络安全工作者们普遍关注的是木马、病毒、挂马、钓鱼等纯粹的民用安全问题。之后是移动互联网、商业网站、商业系统的安全性问题(入侵、篡改、拖库、撞库、个人信息泄露、DDoS 攻击等)。而到了 2015 年，网络安全工作者们最爱谈论的前沿话题是“APT(高级持续性威胁)攻击”。这是一种针对性和隐蔽性极强的网络攻击行为。

本书首先从震网病毒讲起，然后介绍什么是 APT 攻击，以及全球发现的攻击态势、典型的攻击事件和影响，带领读者深入浅出地了解 APT 攻击；再从攻击的技术(包括 APT 攻击的目标与平台、武器搭载系统、软件工具、使用的服务器等)，战术布阵思路，以及攻防的未来发展趋势等方面，进一步地介绍 APT 攻击；最后详细分析了摩诃草、双尾蝎、美人鱼等 APT 组织的攻击全过程。

本书可供政企机构管理人员，安全部门工作者，网络与信息安全相关研究机构研究人员，高等院校相关专业教师、学生，以及其他对网络空间安全感兴趣的读者学习参考。

图书在版编目(CIP)数据

透视 APT：赛博空间的高级威胁/奇安信威胁情报中心著. —北京：电子工业出版社，2019.8
ISBN 978-7-121-37101-1

I. ①透… II. ①奇… III. ①互联网络－安全技术 IV. ①TP393.408

中国版本图书馆 CIP 数据核字(2019)第 144173 号

责任编辑：戴晨辰　　文字编辑：刘　瑀
印　　刷：北京盛通印刷股份有限公司
装　　订：北京盛通印刷股份有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：720×1000　1/16　印张：12.25　　字数：176 千字
版　　次：2019 年 8 月第 1 版
印　　次：2019 年 9 月第 2 次印刷
定　　价：52.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010)88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：dcc@phei.com.cn。

前言

Preface

APT（Advanced Persistent Threat，高级持续性威胁）攻击堪称网络空间中的军事对抗。攻击者会长期、持续地对特定目标进行精准打击。中国也是 APT 攻击的主要受害国之一。绝大多数的 APT 组织具有一定的政府背景，其攻击的战略目标也是以政府、军队、科研机构和大型商业机构为主，而目的则是窃取被攻击组织网络中的敏感情报信息。

事实上，APT 攻击就是一场发生在互联网上的情报战争，而攻防双方的焦点则是情报和信息。当然，在某些特定的情况下，APT 攻击也会瞄准金融机构、工业系统和地缘政治，某些 APT 攻击的影响甚至是世界性的。

2015 年 5 月以来，奇安信威胁情报中心就开始对全球范围内的 APT 组织及其活动展开了持续的监测和深入的研究。本书基于公开威胁情报和自有安全监测分析结果编写，是一本面向政企机构管理人员，安全部门工作者，网络与信息安全相关研究机构研究人员，高等院校相关专业教师、学生，以及其他对网络空间安全感兴趣的读者的科普类读物。全书包括网络空间中的对抗、典型 APT 事件及其影响、APT 组织的技术实践、APT 组织的战术布阵、APT 攻击与防御技术趋势、典型的 APT 组织概述六个部分，从 APT 攻击的发展历史、事件和影响、技术战

术等多个方面，系统地介绍了 APT 攻击的基础知识，希望能够帮助读者全面认识 APT 攻击。

虽然 APT 攻击的手法高深，但本书内容不涉及任何专业的、复杂的技术细节描述，重点介绍主要现象、基本原理和最终结果。作为一本科普读物，读者不需要具备通信、计算机或网络安全方面的专业知识，即可畅读本书绝大部分内容。并且本书用详细生动的内容介绍典型 APT 攻击的事件，通过巧妙的写作手法让一些黑客技术、工具变得有趣、形象，更增加了本书的阅读趣味性，同时也希望能够激发读者对网络安全的兴趣爱好，未来成为网络安全工作者中的一员。

在第一部分，通过震网病毒开篇，介绍了整个攻击的前因后果，让读者快速感知到 APT 攻击的严重后果，再通过系统地阐述 APT 攻击的定义、特点、形式，以及当前国际上对 APT 的研究情况，带领读者初步建立对 APT 攻击的认知。

在第二部分，列举了工业、金融、政治等领域知名的 APT 事件，加深读者对于 APT 攻击破坏性的认知。

在第三部分，从攻击者使用的攻击方法、平台、木马、漏洞、C&C 服务器等角度，进行了全方位的介绍，让读者近距离看清 APT 攻击的特点。

在第四部分，就 APT 组织在实际攻击中所采用的各种战略战术方法展开分析，包括攻击初期的情报收集、火力侦察、假旗行动，攻击过程中的供应链攻击、周期性骚扰，攻击成功后为扩大战果进行的横向移动，以及多种复杂的伪装术、反侦察术等，使读者了解一次 APT 攻击的全过程。

在第五部分，介绍了当前 APT 攻击技术的特点和发展趋势，并针对这些特点和趋势，重点阐述了发现、分析和防御 APT 攻击的技术和方法，以便让读者了解 APT 攻击是可以及时发现和防御的。

在第六部分，详细介绍了全球知名 APT 组织（如方程式、索伦之眼、APT28 等）和国内安全厂商独立发现的 APT 组织（如海莲花、摩诃草、蔓灵花等）的攻击特点及行为特征，帮助读者更加深入地了解 APT 组织及其活动的典型特征。

此外，本书还在附录中总结了 APT 组织的人员构成和命名规则，并揭秘了奇

安信威胁情报中心参与命名 APT 组织时的思路，以飨读者。

最后，特别感谢奇安信集团裴智勇、汪列军、刘洋、潘博文积极组织本书的出版。同时，本书的顺利出版还离不开电子工业出版社戴晨辰编辑的大力支持，以及其他工作人员的辛勤付出，在此向他们一并表示感谢。由于作者水平有限，不妥之处在所难免，恳请网络安全业界专家、广大读者朋友批评指正，共同为我国网络空间安全科普与教育事业贡献力量！

编　者

奇安信威胁情报中心简介

奇安信威胁情报中心是奇安信集团旗下专门从事威胁情报研究、产出及相关产品开发的机构。奇安信威胁情报中心基于奇安信全系列安全产品，以及开源商业数据源中的海量多维度安全大数据，利用机器学习的自动化流程，结合安全专家在威胁对抗方面丰富的实践经验，形成全方位、全链条的威胁情报能力。奇安信威胁情报中心的输出内容包括：战术情报、作战情报和战略情报，赋能安全产品、安全运营/事件响应团队、安全管理者，提升对多种威胁的预防、检测、分析、响应和处置能力。截至目前，奇安信威胁情报中心已累计截获境内外 APT 组织 39 个，率先披露并独立命名 APT 组织 13 个，处于国际 APT 研究前列。

目录

Contents

第一部分　网络空间中的对抗

第二部分　典型 APT 事件及其影响

第三部分　APT 组织的技术实战

第六部分 典型的 APT 组织概述

第一部分 Part 1 网络空间中的对抗

第 1 章

开篇故事：震网病毒

1.1 首个国家级网络武器

谈到 APT(Advanced Persistent Threat，高级持续性威胁)攻击，就不能不提到震网病毒。因为它是全球公认的、世界上第一款军用级网络攻击武器，世界上第一款针对工业控制系统的木马病毒，世界上第一款能够对现实世界产生破坏性影响的木马病毒。

震网病毒是一款蠕虫病毒，其英文名称是 Stuxnet，最早于 2010 年 6 月由白俄罗斯安全公司 VirusBlokAda 发现并披露，而其最早的攻击至少可以追溯到 2009 年 6 月。赛门铁克(Symantec)和卡巴斯基(Kaspersky)等知名安全公司也都曾先后对该病毒进行过深入的追踪与研究。

从扩散的地区来看，震网病毒显然是一款以伊朗为主要攻击目标的木马病毒。赛门铁克和微软的相关研究显示，在已经确认被震网病毒感染的全球超过 45000 个工业控制系统中，近 60% 出现在伊朗，其次为印尼(约 20%)和印度(约 10%)。此外，阿塞拜疆、美国与巴基斯坦等地亦有少量个案发生。而就伊朗本身的情况来看，当时伊朗境内至少有 60% 的个人计算机感染了震网病毒，约有 500 万网民受到了影响。

从攻击原理来看，震网病毒攻击的终极目标是核设施中的离心机设备，这种设备是用来制造核电站燃料“浓缩铀”的。当病毒感染了控制离心机系统的计算机主机(装有 SIMATIC WinCC 系统、西门子视窗控制中心，一般简称 WinCC)后，会首先记录离心机正常运转时的数据，如某个阀门的状态或操作温度，然后将这个数据不断地发送到监控设备上，使工作人员误认为

离心机一直正常工作。与此同时，病毒会控制 WinCC 系统，并向离心机发送虚假的输入控制信号，从而导致离心机运转速度失控，最终达到令离心机瘫痪乃至报废的目的。

从攻击结果来看，伊朗也是损失最为惨重的。2011 年 1 月 16 日，美国《纽约时报》发表文章称，震网病毒于 2010 年 7 月攻击了伊朗核设施，导致其浓缩铀工厂内约 1/5 的离心机报废，从而大大延迟了伊朗的核计划。同年 2 月，伊朗突然宣布暂时卸载布什尔核电站的核燃料，并有消息称，伊朗位于纳坦兹的约 8000 台离心机中有 1000 台在 2009 年年底和 2010 年年初已经被换掉。这些消息也在一定程度上侧面证实了《纽约时报》的说法。

2011 年 8 月，一名伊朗议员对新闻媒体透露，布什尔核电站因为不能按时提供足够的核燃料，无法按计划于当年 8 月底并网发电。2011 年 9 月 4 日，伊朗原子能组织宣布布什尔核电站于当天并网发电，但连网的功率只有约 60 兆瓦，仅为核电站总装机容量的 6%。而俄罗斯常驻北约代表罗戈津则更进一步对外宣称，震网病毒给伊朗布什尔核电站造成严重影响，导致放射性物质泄露，危害不亚于切尔诺贝利核电站事故。

1.2 震网病毒的潜伏渗透

有趣的是，虽然震网病毒的最终攻击目标是工业控制系统，特别是核电站、水坝、国家电网等电力基础设施，但其传播扩散过程却是通过民用个人计算机进行的，并且经过了漫长的潜伏和扩散，才最终成功渗透进入伊朗的核设施中。也就是说，这款病毒虽然感染了大量的普通个人计算机（伊朗境内 60%以上的个人计算机），但却不会对普通个人计算机发动任何显性攻击，而只是静静地把自己隐藏在计算机硬盘中。只有当病毒检测周围环境，并确认自身处于工业控制系统或核设施中时，才会发动破坏性攻击。正是这种奇特的攻击方式，才使其能够在民间广泛传播而长期不被发现。

对目标的精确甄别，恰恰是 APT 攻击与普通民用攻击的一个巨大的区

别。震网病毒之所以会将大量的普通个人计算机变成病毒携带者而不对宿主发动任何显性攻击，一个根本的原因就是想要暗中突破真正攻击目标所处的物理隔离环境。

与全球绝大多数工业控制系统相类似，伊朗的核设施与互联网之间也是相互隔离的，而且是严格的物理隔离——核电站的工业控制系统与互联网之间没有任何物理连接，包括有线连接和无线连接。这使得通过互联网向伊朗的核设施发动远程网络攻击成为一件看起来不太可能的事情。

但有一个重要的元素——U 盘，这种在 21 世纪初已经被普遍使用的移动存储设备，成为病毒的“摆渡”。震网病毒一旦发现个人计算机上插入了 U 盘等移动存储设备，就会将自身在 U 盘中复制一份。而当这个带病毒的 U 盘被插入其他计算机时，病毒就会立即感染其他计算机，并找到新的宿主。这种传播过程不断地在暗中持续，直到有核电站的工作人员不慎将带病毒的 U 盘插入了核电站内部的计算机设备，震网病毒才开始对整个网络中的计算机设备发动破坏性攻击。

除了在宿主机身上的“低调作风”，震网病毒得以成功渗透并发动破坏性攻击的另外一个重要原因就是对“漏洞”的利用。研究发现，震网病毒至少利用了 4 个微软 Windows 操作系统的 0day 漏洞和 3 个西门子工业控制系统漏洞。由于 0day 漏洞在理论上来说是不可防御的，震网病毒也因此实现了难以察觉的自动入侵、快速扩散和恶意控制。

综上所述，震网病毒的整体传播思路是：首先感染外部主机；然后感染 U 盘；再以 U 盘为摆渡，利用系统漏洞传播到工业控制系统的内部网络中；之后再在内部网络中通过多个系统漏洞实现连网主机之间的传播；最后抵达安装了 WinCC 系统的离心机控制主机，并展开攻击。

1.3 震网病毒的身世之谜

目前尚没有任何组织宣称为震网病毒事件负责，但国际舆论和学术界针对此事件仍然有许多观点。

第一，从病毒的设计原理来看，病毒攻击的目的十分明确，并且肯定不是以普通个人为最终攻击目标的。

第二，从病毒的技术水平来看，其代码的规模与复杂程度、漏洞利用的水平(能同时利用多个 0day 漏洞)都远远超越了同时代的其他已知木马病毒，所以很难想象震网病毒出自一般国家政府之手，更别说没有任何政府背景的民间攻击组织。

第三，从病毒攻击的实际结果来看，很有可能是主要受害国伊朗的最主要的敌对政治势力所为。

除了上述几点，近年来，又有越来越多的相关证据被不断地披露。

2015 年，卡巴斯基实验室披露了一个名为方程式(Equation Group)的网络攻击组织，该组织与此前发现的火焰病毒(Flame)及震网病毒(Stuxnet)存在密切联系。

2016 年以来，一个自称影子经纪人(The Shadow Brokers)的攻击组织宣称获得了方程式的网络武器，并不断地在网上公开部分方程式的网络武器代码。根据影子经纪人泄露的相关信息分析，震网病毒确实与方程式有密切的关系。

值得一提的是，2017 年 5 月爆发的震惊全球的永恒之蓝勒索蠕虫(WanaCry)攻击事件中，病毒所使用的高级漏洞攻击武器永恒之蓝，也是影子经纪人所披露的方程式的网络武器之一。

1.4 关于震网病毒的思考

震网病毒事件向全世界展示了一种全新的、国家间的战争形态——网络战争。尽管此前，网络战争的概念早已在各类科幻作品中屡见不鲜，但震网病毒却第一次把这一理论概念变成了现实。此前发生的各种重大网络攻击事件，通常只是破坏网络系统或盗取信息，而不会对现实世界产生实质性的影响，所以也算不上是真正意义的网络战争。但震网病毒让人们亲眼见证了一

场没有硝烟、兵不血刃的战争。其对现实世界的破坏性，丝毫不亚于一般意义的常规战争，甚至更严重。

震网病毒事件也是业界公认的第一起国家级别的军事网络战，它充分体现了 APT 攻击的一些显著特点。

第一是攻击的高级性。震网病毒的攻击水平远超同时代的任何其他木马病毒，0day 漏洞的大量使用使其几乎是不可防御的。

第二是攻击的持续性。震网病毒的攻击至少从 2009 年 6 月就开始了，经过长期的潜伏和渗透，才最终达到了攻击目的，并且其攻击至少持续了一年以上才被发现。而如果再考虑到震网病毒的 C2 服务器(对病毒进行控制的服务器)早在 2005 年 11 月就被注册了，那么震网病毒背后组织的潜伏周期可能长达 6～7 年。

第三是攻击的针对性。震网病毒针对普通的个人计算机只感染不攻击，但对核设施则会进行精心设计的复杂攻击，足见其对攻击目标的精准选择。同时，工业控制系统遍布全球，但却只有伊朗成为重灾区，印尼、印度等国的工业控制系统虽然也有大量感染，但却没有发生太严重的安全事故。这些也都说明，攻击者对病毒的传播过程进行了比较准确的控制。

不过，作为已知的第一款网络攻击武器，震网病毒也带有一些非典型的 APT 特征，特别是其传播过程，仍然带有明显的传统攻击的思维特点，这在后来人们发现的大量其他 APT 攻击中是比较少见的。

震网病毒的传播方式，可以简单地概括为“广泛播种，重点突破”。在攻击真正的目标，即核设施之前，震网病毒首先在普通个人计算机用户中进行了广泛的传播，仅伊朗境内的感染者就可能多达 500 万人以上。如此大规模的网络攻击却在长达一年以上的时间里完全没有被发现，这在今天看来几乎是一个不可思议的奇迹。因此，只能感叹震网病毒作者超越时代的高超技术和异常大胆的战略设想。

但客观来说，“广泛播种”的思想就是一种典型的传统攻击思维方式。