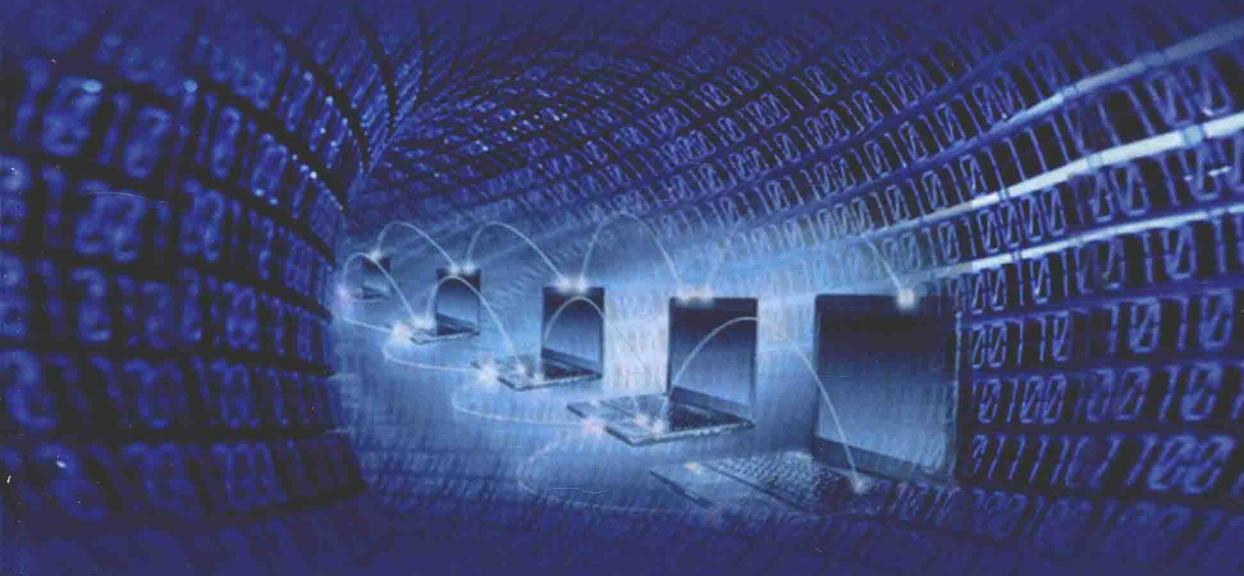
中国国防科技信息中心



# 定向网络攻击

## ——由漏洞利用与恶意软件驱动的多阶段攻击

Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware

[美] Aditya K Sood　Richard Enbody　著

孙宇军　耿国桐　范笑峥　等译

国防工业出版社
National Defense Industry Press

ELSEVIER

ELSEVIER
爱思唯尔

# 定向网络攻击

## 由漏洞利用与[redacted]阶段攻击

**Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware**

[美] Aditya K Sood　Richard Enbody　著
孙宇军　耿国桐　范笑峥　等译

国防工业出版社
·北京·

著作权合同登记　图字: 军 -2015 -032 号

**图书在版编目（CIP）数据**

定向网络攻击: 由漏洞利用与恶意软件驱动的多阶段攻击/(美) 阿迪蒂亚·苏德 (Aditya K Sood), (美) 理查德·尹鲍德 (Richard Enbody) 著; 孙宇军等译. — 北京: 国防工业出版社, 2016. 7
（国防科技译丛）
书名原文: Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware
ISBN 978-7-118-11049-4

Ⅰ. ①定… Ⅱ. ①阿… ②理… ③孙… Ⅲ. ①网络攻击—研究 Ⅳ. ①TP393.081

中国版本图书馆CIP数据核字 (2016) 第 196254 号



※

国防工业出版社出版发行
(北京市海淀区紫竹院南路 23 号　邮政编码 100048)
国防工业出版社印刷厂印刷
新华书店经售
*

**开本** 710 × 1000　1/16　**印张** 10　**字数** 118 千字
2016 年 8 月第 1 版第 1 次印刷　**印数** 1—2000 册　**定价** 48.00 元

**(本书如有印装错误，我社负责调换)**

国防书店: (010) 88540777　　发行邮购: (010) 88540776
发行传真: (010) 88540755　　发行业务: (010) 88540717

# “国防科技译丛”序言

当今世界，国际安全格局正酝酿重大变革，大国军事力量转型加快，新兴战略空间竞争激烈，新型作战武器层出不穷，前沿颠覆技术屡有突破，创新军事理论不断涌现，新一轮科技革命、产业革命和军事革命正在到来。为帮助广大读者深入了解世界国防科技的发展态势，准确把握军事技术前沿的发展动向，我们组织国内专家学者推出了“国防科技译丛”系列产品。

本译丛面向国防科技建设全领域、全要素、全过程，突出“创立品牌、服务高端”目标，覆盖军事理论、军事战略、国防采办、武器装备、军事技术、科技管理、试验鉴定、军控军贸、基础技术等领域，精选翻译具有权威性、战略性、学术性的当代国外政府报告、学术专著和智库成果。

由于立场不同，丛书中部分观点未免有失偏颇，读者在阅读时应注意辩证分析，择善而用。“知己知彼，百战不殆”，希望本译丛对广大读者有所裨益。同时，也恳请读者惠赐宝贵意见，让“国防科技译丛”越办越好。

中国国防科技信息中心　主任 刘林山

# 定向网络攻击

## 由漏洞利用与恶意软件驱动的多阶段攻击

## 译校者


翻　　译　孙宇军　赵睿涛　谭玉珊　李　璜

审　　校　范笑峥　夏文成　李耐和　陈茂良

审读校订　耿国桐　陈　豫　刘雪奎　朱　松

# 概述

本书讨论了定向攻击和网络犯罪的机理。该书的写作目的是针对定向攻击发生过程中的不同阶段, 通过提供系统和分层次的模型, 让用户掌握有关定向攻击的知识。定向攻击的每一个步骤, 都将在独立的章节详细介绍, 诠释其隐秘的过程, 并讲述攻击者是如何成功实施的。各章节内容如下:

• 第 1 章介绍了定向攻击这一主题, 对定向攻击的完整模型和目的进行了解释。本章描述了成功实施定向攻击所需的不同阶段。读者将会对定向攻击的基本模式有一个总体了解, 包括情报搜集、感染目标、系统漏洞利用、数据泄露和对目标网络的持续控制。本章还揭示了定向攻击和先进持续性威胁之间的区别。

• 第 2 章揭示了攻击者采用的不同类型的情报搜集步骤, 如开源情报、网络空间情报 (CYBINT) 和人力情报 (HUMINT) 以及这些情报之间的关联。本章讨论了攻击者在执行某一类侦察前如何利用互联网及来自在线社交网络、网站、杂志等不同信息源中有关个人和机构的公开资料搜集目标情报。搜集的目标信息决定了定向攻击的方向。

• 第 3 章讨论了攻击者用来感染目标, 使其下载恶意软件并破坏系统的各种策略。本章讨论了使用最为广泛的定向攻击策略, 如 “鱼叉式网络钓鱼” (spear phishing)、“水坑” 式攻击 (waterholing)、自带办公设备 (BYOD) 感染模式, 以及通过利用网络和软件漏洞进行的直接攻击。感染目标的唯一动机是寻找漏洞, 以植入恶意软件从而实现对目标系统的完全控制。每种攻击模式都对应一个触发定向攻击的路径。

• 第 4 章揭示了系统漏洞利用的完整细节, 涵盖了破坏系统所使用

的不同类型漏洞和弱点。本章介绍了供应商设计的针对不同保护机理的分层布局, 以及攻击者如何绕过这种保护机制成功发动攻击。详细描述了绕过数据执行保护 (DEP) 和地址空间布局随机化 (ASLR), 包括利用漏洞的写入机制, 如面向返回的编程 (ROP) 和重要信息泄露漏洞。本章还涉及由相关公司设计的旨在破坏攻击者利用漏洞写入的不同安全解决方案。另外, 还详细介绍了高级恶意软件及其基本运用技巧, 这些技巧往往能规避信息安全人员的安全设计。

• 第 5 章介绍了可被攻击者选定的数据泄露机制, 使其能够从受感染的系统中提取数据。数据泄露包括两个阶段, 即数据窃取和将数据传输到由攻击者控制的服务器。讨论了 Web 注入、窃取视频和截图、表单抓取、操作系统信息窃取等采用不同策略的传输方式, 如加密、不同协议的信道压缩比 (例如 HTTP/HTTPS、点对点 (P2P) 和互联网中继聊天 (IRC))。总体而言, 这一章描述了定向攻击中使用的复杂数据泄露模式。

• 第 6 章揭示了攻击者使用的各种用于保持对目标控制并在网络中长期潜伏的技术。攻击者不断侦察网络以求影响并破坏网络中更多的系统, 使信息可以大规模地泄露。攻击者使用定制、自制和公开可获得的工具, 如远程访问工具包 (RAT) 来执行不同任务, 如扫描端口和利用目标网络的弱点。就长期、不被探测地执行定向攻击而言, 这一步至关重要。

• 第 7 章介绍了犯罪软件服务 (CAAS) 模式通过简单方法构建定向攻击的重要性。总体而言, 本章展示了通过支付一定费用购买不同软件组件以及其他组件, 如遭破坏的托管服务器是非常容易实现的。还讨论了电子货币交易在互联网地下市场中的作用及过程。

• 第 8 章专门讲述针对定向攻击构建多层防御。防御层包括以用户为中心的安全性、端系统安全性、易损性评估和补丁管理、网络监控以及强大的应急预案。本章还介绍了构建下一代防御以应对不断发展的

先进恶意软件的必要性及重要性。

• 第 9 章通过破除一些定向攻击 “神话” 对全书进行了总结, 定义了这些攻击的真正本质。

在本书中, 我们将 “定向网络攻击” 简称为 “定向攻击”。

# 致谢

感谢我的父亲、哥哥和其他家人。感谢我的导师对我持久的支持与鼓励。感谢我妻子的支持。本书献给我刚出生的儿子。

阿迪蒂亚 · 苏德博士

感谢 Aditya 鼓励并鞭策我完成本书。同样, 感谢我的妻子为本书出版所付出的时间。

理查德 · 尹鲍德博士

向安全研究领域所有成员在与网络犯罪和定向攻击斗争中所作出的巨大贡献致以崇高的敬意!

# 作者简介

阿迪蒂亚·苏德博士是一名高级安全研究员和咨询师。苏德博士感兴趣的研究领域包括恶意软件的自动化与分析、应用安全、安全软件设计和网络犯罪。他参与了大量与渗透测试、产品/设备安全、网络、移动和Web应用程序有关的项目，同时服务于IOActive、毕马威等世界财富500强客户。他也是SecNiche安全实验室的创始人之一，这是一个供安全业界共享研究成果的独立门户网站。他在IEEE、Elsevier、CrossTalk、ISACA、Virus Bulletin、USENIX等多种杂志和期刊上发表论文多篇，包括美联社、福克斯新闻、《卫报》、商业内幕、加拿大广播公司在内的多家媒体都报道过其作品。苏德博士也是一位行业会议的积极参与者，在DEFCON、HackInTheBox、黑帽军火库、RSA、《病毒公报》、OWASP等会议上做过报告。他获得了密歇根州立大学的计算机科学博士学位。

理查德·尹鲍德博士是明尼苏达州立大学计算机科学与工程系副教授。1987年他从明尼苏达州立大学获得计算机科学博士学位后留校任教。尹鲍德博士在明尼苏达州诺斯菲尔德的卡尔顿数学学院获得学士学位，从1976年开始，在佛蒙特州和新罕布什尔州执教了6年高中数学。尹鲍德博士在多个领域都发表过研究论文，主要集中在计算机安全和计算机体系结构领域。

# 目录

# 第 1 章　导论

当前, 利用网络和技术进行信息搜集在国际互联网上非常普遍, 定向网络攻击成为一种破坏国际互联网完整运行的常见武器。这些攻击窃取知识产权, 实施网络间谍活动, 损害关键基础设施, 同时给用户带来不确定性。它们可以在互联网上实现战术和战略目标, 而不会带来任何实体上的破坏。很显然, 定向网络攻击提供了一种战术优势, 能够在未来网络战中发挥重要作用。

今天, 大多数国家都在发展网络战能力。对关键软件的 "零日漏洞攻击" (即针对软件开发商还未发觉、也无修补程序可用的未知弱点而设计的攻击) 被认为是可以用于破坏或控制对方网络基础设施的攻击武器。政府安全部门投入数百万美元挖掘 "零日漏洞"。美国政府是这些网络武器的最大买家之一[1]。事实上, 正规的安全公司也会挖掘漏洞、编写零日漏洞攻击软件并出售给政府以获利。这使得国家具备了开展定向网络攻击的实力。此外, 即使掌握了零日漏洞, 发动一次精心策划的定向网络攻击也代价不菲, 因为要针对攻击途径构建多层模式并使其适应目标网络环境。然而, 定向网络攻击背后并不一定都有国家支持, 遍布全球的独立攻击者也可以发起这样的攻击。

定向网络攻击的影响和能力很容易被低估。它们足以形成动能效应, 即通过执行远程攻击者的命令对目标的实体基础设施造成破坏。以工业控制系统 (ICS) 为攻击目标的 "震网" (Stuxnet)[2] 就是这样的实例。ICS 是一种控制系统, 用于控制和指挥包括油、气、水、电等产业 (关键基础设施) 使用的机器 (设备)。设计精良的网络攻击可以作为摄

取目标关键信息的“寄生虫”。定向网络攻击的作用与其在目标网络中的持久性和隐蔽能力直接相关。要在具备网络弹性和对抗策略的敌对环境中取得成功，定向网络攻击需要多阶段的攻击途径，构建一个相互叠加的攻击模式。另一方面，自动入侵预防技术需要具备评估并描绘定向网络攻击概率和后果的能力。

定向网络攻击有几种定义。根据命名规则，我们采用其中一种基本的定义，即定向网络攻击是针对特定用户、公司或组织，以隐蔽方式获取关键数据的一种攻击行为。定向攻击不应与本质上随机的泛攻击相混淆，泛攻击主要感染并影响较大的用户群。定向攻击的鉴别关键是本质上不随机。这意味着定向攻击的攻击者能够区分目标（系统/用户/机构），并伺机执行攻击计划。然而，“定向攻击”这个术语已被滥用。我们认为，定向攻击的最佳模式包括不同的组成部分，在五个阶段执行隐秘行动：情报搜集、目标感染、系统漏洞攻击、数据泄露以及保持控制。情报搜集阶段包含攻击者为获取目标数据而使用的不同信息搜集策略。感染目标阶段揭示了目标是如何被携带病毒的恶意软件所感染的。系统漏洞利用阶段展示如何利用漏洞攻击彻底破坏系统。数据泄露阶段即从被感染系统中提取信息。保持控制阶段展示了攻击者如何在网络中保持持久隐身，以及如何进入目标环境中的其他系统。

定向攻击的重要特点如下：

- 使用针对未知弱点的“零日漏洞攻击”破坏目标系统，以确保攻击不易被察觉。
- 使用复杂的恶意软件系列（自定义编码），即使网络和终端用户系统中安装有安全解决方案，往往也不会被察觉。
- 隐藏攻击者的真实身份，保持低姿态以避免法律问题。
- 在攻击行动中，没有价值的系统不会被感染和破坏，从而降低了攻击的曝光程度，使其更具隐蔽性。
- 攻击周期长，并且以隐蔽的方式进行。