 DOI: https://doi.org/10.12349/iser.v4i2.1224

Research on the Application of Network Killing Chain Model in Network Attack and Defense

Dechun Zhao

Network Information Center of Kunming Vocational and Technical College of Industry, Kunming, Yunnan, 650302, China

Abstract

The essence of network security is offensive and defensive confrontation. The network killing chain is a commonly used model for active attacks by network attackers, and it is a security model that describes the various stages of network attacks. This model helps to understand and analyze each stage of network attacks. In the battle of network attack and defense, this model can be used by attackers for network attacks, and defenders can also be used for network defense. Therefore, studying the network kill chain model helps us to familiarize ourselves with the steps and operations of network attacks, select the correct tools and strategies to detect malicious intruders to limit their violations, more effectively respond to complex attack behaviors such as ransomware and APT, and minimize the risk of network attacks, to ensure the normal operation of the enterprise's network.

Keywords

network killing chain; network attacks; network defense; terms of settlement

网络杀伤链模型在网络攻击与防御中的应用研究

赵得椿

昆明工业职业技术学院网络信息中心，中国 · 云南 昆明 650302

摘　要

网络安全的本质是攻防对抗。网络杀伤链是网络攻击者进行主动攻击的常用模型，是描述网络攻击各个阶段的安全模型，该模型有助于理解和分析网络攻击的每个阶段。在网络攻防较量中，该模型攻击者可用于网络攻击，防御者也可用于网络防护，所以研究网络杀伤链模型有助于我们熟知网络攻击的步骤和操作，从而选择正确的工具和检测恶意入侵者的策略来限制其违规行为，更有效地应对勒索软件和APT之类的复杂攻击行为，并将最大限度地降低网络攻击的风险，为企业的网络正常运行保驾护航。

关键词

网络杀伤链；网络攻击；网络防御；解决办法

1 引言

随着无处不在的网络，网络攻击已经呈现出常态化和复杂化。网络安全是围绕攻防对抗模型构建起来的应用型学科，哪里有用户，哪里有数据，哪里就有安全问题。而网络攻防对抗又是一个持续对抗的动态过程，防御方必须使用主动防御和动态防御的策略才能与攻击方抗衡。网络杀伤链的英文是 Cyber Kill Chain，也称为网络攻击生命周期或网络攻击链，是 2011 年由美国航空航天制造商洛克希德 · 马丁公司开发的网络攻击模型。该模型对大量网络攻击，特别是 APT 类攻击案例的分析，从攻击者的角度以分段式描述和拆分了网络攻击者对网络入侵的每个阶段，链条中的所有环节环环相扣，一环脱节，全盘皆散，因此要保证每个阶段都成功才能保证整个攻击实现。防御者可以使用该模型来检测识别和防止网络入侵，包含从早期的计划和监视到网络攻击成功。

“杀伤链”又称“动态目标指示”，来源于军事领域，是把打击一个动态目标的过程分解为由“发现—定位—跟踪—瞄准—打击—评估（Find、Fix、Track、Target、Engage、Assess）”六个环节相扣而构成的阶段模型，即包括目标的识别、向目标派遣部队、发送打击目标的命令和目标的消除，也可以用来反制此类攻击（反杀伤链）。在越早的网络杀伤链环节阻止攻击，越可能被阻止，修复的时间和成本也就越小，防护的效果就越好。例如，攻击者获取的信息越少，利用这些信息完成攻击的可能性也就越小。如果网络攻击直到进入单位网络中才被阻止，那么企业可能就不得不修复服务器，并进行大量的取证工作核验被泄露的信息。

【作者简介】赵得椿（1982–），男，中国云南泸西人，硕士，副教授，从事网络空间安全研究。

2 传统网络攻击模型

2.1 基于树结构的网络攻击模型

基于树结构的网络攻击模型是 Schneier 在 1999 年提出的一种系统攻击分类方法，它起源于故障分析方法，后来扩展为软件故障树，用 AND-OR 形式的树结构对目标对象进行网络安全威胁分析。攻击树方法可以被网络攻击者用来进行渗透测试，也可以被防御者用来研究防御机制。该模型能够采取专家头脑风暴法，并且将这些意见融合到攻击树中去，进行费效分析或者概率分析，可以对非常复杂的攻击场景建模。但是由于树结构的内在限制，攻击树不能用来建模多重尝试攻击、时间依赖及访问控制等场景，也不能用来对循环事件建模，对于现实中的大规模网络，攻击树方法处理起来也很复杂 [1]。

2.2 基于图结构的网络攻击模型

基于图结构的网络攻击模型是 Phillips 和 Swiler 在 1998 年提出的一种系统攻击分类方法，是目前应用最广的网络攻击模型。它从攻击者的角度出发，在综合分析多种网络配置和脆弱性信息的基础上，找出所有可能的攻击路径，并提供了一种表示攻击过程场景的可视化方法，从而帮助网络安全管理人员直观地理解目标网络内各个脆弱性之间的关系、脆弱性与网络安全配置之间的关系以及由此产生的潜在威胁。攻击图以图形化的方式展示了网络中所有可被防御方发现的攻击路径。对目标网络构建攻击图，一方面可以分析从边界节点到需要进行重点保护节点可能的攻击路径，对路径上的高危节点进行重点防御，达到保护重要节点的目的；另一方面可以在攻击发生时实时分析攻击者的攻击能力和推断攻击者的后续攻击目标，以便采取应对和反制措施。

2.3 基于网结构的网络攻击模型

基于网结构的网络攻击模型是 Kumar 和 Spafford 在 1994 年采用 Petri 网进行安全建模。2001 年 McDermott 提出基于 Petri 网的网络攻击模型，后来经过许多专家不断改进，提出基于时间 Petri 网的模型、基于 WiKiWeb 的攻击网。它以 Petri 网为基础，理论丰富，描述能力强，便于精确分析，适合描述协同网络攻击，但是很难适应复杂的网络攻击行为 [2]。

3 网络杀伤链在网络攻击与防御中的应用

网络杀伤链用来拆分任何恶意软件攻击的每个阶段，从而达到识别和阻止网络攻击。如果防御者能够成功阻止某一阶段的攻击，那么攻击者下一个阶段的攻击活动将会受到相应的限制。但是，攻击策略是可以改变的，所以网络攻击与防御双方是一个动态、永恒的较量。网络杀伤链模型分为七步，如图 1 所示。

在这七个步骤中，目标侦察跟踪属于预利用阶段；武器构建、载荷投递、漏洞利用、安装植入和命令与控制属于利用阶段；执行任务属于利用后期阶段。

第一步：Reconnaissance 即目标侦察跟踪：从外部全方位研究受害者。

网络攻击者根据攻击目的对目标的识别和选择，从各种渠道尽可能多地搜集攻击目标的信息对其进行深入研究，绘制目标画像和拓扑结构，寻找目标的弱点或不当配置，以便后期通过制定入侵策略直击目标最脆弱的地方，具体手段如收集钓鱼攻击使用的登陆凭证和相关信息（见表 1）。

第二步：Weaponization 即武器研制与构建：磨刀不误砍柴工，使用漏洞和后门制作一个可发送的武器载荷。

“工欲善其事，必先利其器”。攻击者根据侦察过程中收集和分析的信息，根据入侵的目的和目标对象的特点，利用“传统兵器”，打造“特种兵器”，构建有针对性攻击的“武器库”。将具有远程访问功能的木马与漏洞利用工具相结合，形成可投递攻击的载荷，根据目标对象的漏洞和后门制作一个可发送的武器载体，如编写各种工具、后门、病毒、Exp、Weapon 和 Malware，经常是一个包含有恶意代码的 PDF 文件或 Office 文档 [3]，见表 2。

第三步：Delivery 即载荷投递：向目标投递武器化的工具包。

将构建的攻击载荷或武器化的捆绑包向目标投递，如通过水坑、鱼叉等攻击方式将武器散播出去，经常是发送一封带有恶意链接的欺诈邮件或者使用钓鱼网页和通过移动存储介质传播病毒，见表 3。

第四步：Exploitation 即漏洞利用：利用漏洞在受害者的系统上运行代码。

网络边界在这里被破坏。通过漏洞利用过程触发精心构建的攻击代码使其在受害者的系统上运行，并获取对对方的控制，经常使用安装工具、运行脚本、动态数据交换、本地作业调度和修改安全证书等来利用目标系统。经常使用安装恶意软件或反向 shell 程序，从而远程可以不受限制地访问目标网络 [4]，见表 4。

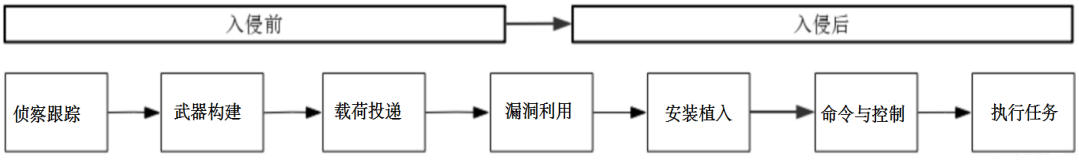

图 1 “网络杀伤链”模型

表 1 目标侦察跟踪

	攻击方	防御方
特点	属于攻击方的计划阶段。根据攻击目的从外部了解企业的资源和网络环境，进行广泛收集信息，寻找可能目标、对特定目标有针对性的深入研究，识别和确定攻击对象，使他们的攻击目的能够实现自己的目标，并评估攻击成本。攻击者希望在此阶段访问系统表，以便搜索组织中的数据库，甚至修改数据库权限，其目标是尽可能多地获取有关数据或资产的信息。攻击者希望目标防备薄弱，数据价值高	属于网络攻击的初级阶段，它的反探测侦察非常艰难，使用机器学习、大数据分析和人工智能等方式能发现部分网络侦察行为。 检测：网络分析；网络入侵检测系统 拒绝：信息共享政策；访问控制列表
常用方式	攻击者经常采用：社会工程学、网络扫描和嗅探、主机检测、服务器枚举、网络拓扑映射、ACL 和包过滤检测以及操作系统指纹识别、漏洞探测、BGP 查询、资产扫描、代码搜索、关键人物识别和防护能力识别来搜集目标的信息。 通过 Google hacking 或爬虫工具收集目标组织和个人暴露在网站、社交媒体上的敏感信息，如企业架构、员工电子邮件、热点研究方向、采购信息、新闻稿、参加会议的名单，泄密文件等； 通过 Shodan、Zoomeye 等网络空间资产探测工具收集目标的互联网资产信息，如在线设备、网站、服务器情况、应用系统及其使用的服务和组件等信息； 通过站长工具、爱站、微步在线等工具查询目标的 whois 信息，包括目标相关域名的 IP 以及所有者信息等； 通过 Nmap、Ping、Nslookup 等工具自动扫描或暴力密码查找系统中的漏洞，收集目标网络空间资产的状态信息、属性信息、关联信息等，以期获得攻击入口点。 通过 Github、GitLab、BitBucket 等源代码托管平台，收集目标及其关联系统的源码信息； 利用社会工程学方法，通过客服电话、人员潜入、社工库查询等方式，获取目标组织的相关信息； 查看目标环境的防御设备部署情况	汇总网站访问日志警报和历史搜索记录，对网络流量进行威胁分析； 修改网站错误回显信息避免暴露服务器情况，利用基线核查工具或漏洞扫描工具，定期对服务器安全性进行评估和加固； 收集设备和系统的日志，建立浏览异常、行为独特的检测机制，重点是基于技术和人的反侦察活动； 不在公开网站上暴露组织的敏感信息；利用互联网敏感信息检测工具，定期检测暴露在互联网上的敏感信息并及时处理，收敛信息暴露面； 加固服务器配置，关闭不必要的端口和服务，对操作系统和软件及时安装补丁或更新包，减少系统攻击入口点和攻击向量； 在网络边界部署 WAF、入侵防御、下一代防火墙等安全防护设备，有效抵御扫描器、网络爬虫等攻击和加固网络边界安全； 部署蜜罐网络，混淆攻击者的侦测目标，主动识别攻击者身份，对入侵者进行 IP 溯源追击； 采用 UEBA 的分析方法，发现潜在的威胁者； 使用其他手段在网络攻击的开始阶段拖延入侵进度，限制攻击手段，增加攻击者的入侵成本，让攻击者知难而退

表 2 武器研制与构建

	攻击方	防御方
特点	这是攻击方的准备工作阶段。攻击方根据目标的漏洞扫描和防护措施确定攻击方式，制作定向攻击武器。利用混淆、加壳、加密等技术制作变种恶意程序，利用 AI 技术 Bypass 动态检测和自学习攻击模型进行情报库污染等试图减少被组织的安全解决方案检测到的机会。通过后门将漏洞利用耦合到可交付的有效载荷中	在攻击发起之前不能有效检测到攻击部署的发生过程，但是可以通过威胁情报跟踪和网络入侵检测系统来进行持久和弹性的防御。 检测：威胁情报；网络入侵检测系统 拒绝：网络入侵防御系统
常用方式	攻击者在该步骤中经常使用：防护规则测试、木马免杀、钓鱼平台、分布式爆破、验证码识别、CC 服务器和远控开发来达到此阶段的目的。 使用 Metasploit 编写有针对性的攻击脚本； 使用 Exploit Pack 库的漏洞利用工具包； 准备僵尸程序、特洛伊木马、网络蠕虫等恶意攻击程序； 根据社会工程学的攻击原理制作钓鱼网站、弱口令库； 准备 SQLMap、BurpSuite、AWVS、WAPITI、中国菜刀、中国蚁剑等常用攻击工具； 制作智能攻击脚本，通过调用工具集实现自动化攻击	使用漏洞扫描工具，及时发现操作系统和应用程序的漏洞，并及时修补漏洞和更新应用程序； 采用网页过滤和电子邮件过滤防止组织用户被水坑式和鱼叉式钓鱼； 安装杀毒软件，对企业重要资产进行定向防护； 利用网站监测工具对钓鱼网站进行定位打击； 开启 WAF、防火墙等产品的攻击防护策略，阻断扫描、注入、拒绝服务、暴力破解等入侵行为； 分析恶意软件，研究其工作原理和软件开发者行为习惯及模式

表 3 载荷投递

	攻击方	防御方
特点	攻击方向目标范围用户投递已经生产好的恶意软件，使其员工收到伪造的内部邮件，邮件的附件包含 Word 伪装的、已做免杀处理的 exe 程序，开始执行攻击行为	这是防御方阻止入侵的第一个，也是最有效和重要的机会。这个阶段也是衡量一个企业的网络安全有效性的重要指标，能否在该阶段进行有效拦截，以阻止入侵尝试和工具传递是很重要的。 检测：端点恶意软件保护 拒绝：变更管理；应用白名单；代理过滤器；基于主机的入侵防御系统（HIPS）
常 用方式	攻击者在该步骤中经常使用：应用交互、钓鱼邮件、供应链投毒、接入办公区和信任网络投递来达到此阶段的目的。 通过 U 盘、硬盘等存储工具，将恶意代码感染至目标主机； 通过钓鱼电子邮件、Web 挂马和即时通信软件等方式将武器化软件包采用“鱼叉式”或“水坑式”钓鱼投递到受害者主机上； 通过应用程序和网络的漏洞，将恶意代码投递至目标主机	安装主机防护软件，检测通过物理介质传输的恶意代码； 在组织的网络边界安装防护软件，分析载荷投递的手段，及时发现并阻断病毒和恶意软件的感染行为； 部署邮件安全网关，识别电子邮件中的恶意文件和高危链接，有效防范通过电子邮件的攻击； 增强单位人员的网络安全意识，能识别一般的网络欺骗行为； 收集攻击者网络入侵的痕迹，用于未来可能出现的司法活动

表 4 漏洞利用

	攻击方	防御方
特点	攻击方利用系统漏洞和被攻击者的安全意识不足进行攻击来获得系统访问权限，以获得敏感数据，如密码文件、数字证书和令牌。经常是员工打开了 exe 程序，其释放了一系列恶意程序，包括计划任务文件、伪装的木马等	系统已经遭到破坏，数据处于危险之中。防御方需要全方位利用加固措施增加防护的弹性，通过以纵深防御思路为基础的框架，增加补偿性安全措施，对重要资产进行防护。 检测：端点恶意软件保护；基于主机的入侵检测系统 拒绝：安全密码；补丁管理
常用方式	攻击者在该步骤中经常使用：口令破解、漏洞利用、信息重复利用、认证绕过和门禁破坏来达到此阶段的目的。 利用漏洞在受害者的系统中执行代码，经常采用基于服务器的安全漏洞，如 SQL 注入、XSS、弱口令、任意文件上传、任意代码上传和缓冲区溢出； 尝试利用员工账号爆破 VPN 系统； 绕过 WAF 的防护利用漏洞； 根据社会工程学让受害者触发漏洞，如点击恶意电子邮件和恶意链接； 人工注册应用系统账号来挖掘系统漏洞，以期寻找入侵点	根据最小权限原则、权限冲突和约束机制进行攻击面管理； 安装杀毒软件和漏洞扫描程序，对软件的行为进行跟踪、研判，对恶意软件及时进行拦截和查杀； Web 开发人员的安全编码培训，提高交付软件的安全性； 用户安全意识培训； 利用沙箱工具，检查未知文件的安全性，动态分析文件行为，深度鉴别文件的危害性； 部署安全防护产品，防止利用常见安全漏洞发起的攻击，拦截远程执行的恶意代码，自定义端点规则阻断 shellcode 执行； 定期举行内部和外部渗透测试，加强端点防御措施； 监控用户账户的权限，如有异常及时修复

第五步：Installation 即安装植入：在目标位置安装恶意软件。

恶意软件使入侵者在远程目标上获得了系统控制权后，安装后门或远程访问木马，提供对入侵者的访问权限，使其可以获得持久化远程访问，见表 5。

第六步：Command and Control 即命令与控制（C&C）：威胁已将变成现实，为攻击者建立可远程控制目标系统的通道。

目标主机向外连接互联网上的命令与控制服务器 C&C 或僵尸网络的主控机，为攻击者建立可远程控制目标系统的命令通道，使其能够远程操纵受害者，对目标主机进行持久化控制，见表 6。

第七步：Actions 即执行任务：通过完全访问和通信，攻击者远程操控实现其预期目标。

攻击者通过一系列攻击活动来破坏系统正常运行和窃取数据，开始侵犯系统的保密性、完整性和可用性，对敏感数据进行窃取、加密、篡改、销毁和入侵其他目标等。攻击者经常利用该主机作为跳板进行横向渗透，扩大攻击面，在局域网中遍历更多的资产，见表 7。

网络杀伤链模型是根据网络攻击与防御而提炼出的框架模型，能比较直观的展示攻击者实施攻击的逻辑思维。企业只有围绕该框架设计防御流程和安全策略，以情报收集和安全分析能力作为基石，防守方才可以利用有利条件转化为防守优势，形成弹性防御，尽量在靠前的阶段上阻止攻击。理想情况下，企业应该在网络杀伤链的前半部分识别并阻止威胁，否则后期成本和风险将更大。当然，攻击者不一定严格按照杀伤链来进行网络攻击，他们可能会实行跳过步骤、添加步骤，甚至重复前面的步骤，特别是一些勒索病毒和 APT 攻击更是如此，因为只有这样它才能绕过组织的防御体系 [5]。

表 5 安装植入

	攻击方	防御方
特点	攻击者能绕过安全防护软件在目标服务器和客户端上安装后门、木马等恶意软件，以便长时间访问攻击目标，并在组织资产上创建持续运行的服务和进程	使用端点防御软件检测和记录“异常”安装活动，分析恶意软件所需的最小权限。 检测：安全信息和事件管理（SIEM）；基于主机的入侵检测系统 拒绝：权限分离；强密码；双因素身份验证
常用方式	攻击者在该步骤中经常使用：写入木马、隐藏文件、隐藏进程、自启动和制作凭证来达到此阶段的目的。 在 web 服务器上安装 webshell 获取用户控制权； 在服务器上部署后门工具、键盘 / 鼠标捕获工具等	使用上网行为管理软件监控系统日志，对于异常文件的创建、修改注册表、调整安全配置、添加删除账户、修改权限、安装远程工具等敏感操作进行管控和审计； 在检测到恶意软件时告警，并进行拦截，对可执行文件进行签名管理； 利用漏洞扫描工具，定期检查系统是否被植入后门，及时查杀后门程序和修复漏洞； 定期备份系统，当系统被入侵后可以恢复到正常状态

表 6 命令与控制

	攻击方	防御方
特点	属于网络攻击的实质性阶段。攻击者通过恶意软件打开通信信道，可以远程控制组织的系统和网络	是防御方进行拦截的最后一个机会，只有对 C&C 操作进行阻止，让攻击者无法向目标物的恶意软件发出指令，才能阻断攻击。 检测：网络入侵检测系统；基于主机的入侵检测系统 拒绝：防火墙访问控制列表；网络分割
常用方式	攻击者在该步骤中经常使用：端口复用、前置代理、自定义协议、通信加密和 udp 协议来达到此阶段的目的； 攻击者经常利用 web、电子邮件和 DNS 协议进行隐藏真实身份； 采用跳板的方式，通过级联的受害者链进行远程控制； 攻击者获得特权账户的访问权限并尝试暴力攻击、搜索凭据并更改权限以接管控制权	部署专业的木马蠕虫检测设备，检查网络中的僵尸主机和受控资产，阻断失陷主机与僵尸网络的 C&C 通道； 部署非法外联检测设备，识别网络中的异常通信，及时警报或阻断未经授权的连接； 使用白名单 / 黑名单机制加强网络访问控制； 规范网络代理协议和代理模块的使用，如 http、DNS； 防御 DNS 穿透和域名服务器毒化； 发现和研究新的 C&C 攻击方式，及时反制

表 7 执行任务

	攻击方	防御方
特点	通过“手敲键盘”的形式，入侵者达到其初始目标，对受害者的访问时间越长，受害者的损失就越大； 攻击者从失陷环境中收集、加密和提取机密信息	监控网络流信息，分析网络通信状况，检测数据泄露和横向移动，对异常数据流，抓包捕获，进行通信量分析； 检测：端点恶意软件保护 拒绝：静态数据加密
常用方式	攻击者在该步骤中经常使用：目标扫描与搜索、数据传输、业务控制、敲诈勒索和清理攻击痕迹来达到此阶段的目的。 破坏受害者的网络与信息； 盗取用户凭证和业务信息、盗用受害者的身份进行活动，通过提升权限进行更深入的活动，以此作为跳板进行横向渗透	根据国家信息系统等级保护制度对信息系统采取分级分域安全管理，做好网络域与域之间的安全隔离，级与级之间的访问控制，防止攻击面被扩散； 健全数据的安全管理制度，部署数据防泄漏产品，严格控制数据访问权限，阻止数据被窃取和横向传输； 健全网络的安全应急响应机制，针对突发的网络安全威胁事件快速定位，缓解并根除攻击； 加强组织的网络空间测绘和网络资产攻击面管理； 对重要业务有灾备方案，面对不可逆转的破坏具备恢复能力，及时修复业务； 对攻击事件采集日志和数据流，为司法取证收集信息

诚然，网络杀伤链模型是链式结构，有不可逆转的趋势，但是使用的一些技术可能在很多地方出现，这也符合迂回战术的特点，特别是提高组织内网络用户的信息安全素养会伴随着网络攻击的任何一个阶段而进行。

4 结语

在网络安全的攻防对抗中，归根结底是“人与人”的对抗。攻击者可能来自任何时间、任何地点、采用无限手段，从任意方向突破和入侵。而防守者则必须时刻保持警惕，全方位布防、持续监控、有效抵御攻击者无孔不入的侵犯。通过在网络攻防对抗中的平衡，攻击者帮助企业被动发现操作系统、应用程序和人性管理的漏洞，促使防御者修复技术和管理方面存在的问题，最终帮助企业构建弹性、纵深的安全解决方案，提高网络安全建设和管理的能力，为组织打造一个固若金汤的网络。

参考文献

[1] Hutchins EM, Cloppert MJ, Amin RM. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains[J]. Leading Issues in Information Warfare & Security Research,2011,1(1):80.

[2] 刘文彦,霍树民,陈扬,等.网络攻击链模型分析及研究[J].通信学报,2018,39(Z2):88-94.

[3] 平国楼,叶晓俊.网络攻击模型研究综述[J].信息安全研究,2020(12).

[4] 马多贺.网络空间欺骗构筑欺骗防御的科学基石[M].雷程,译.北京:机械工业出版社,2017.

[5] 奇安信安服团队.应急响应网络安全的预防、发现、处置和恢复[M].北京:电子工业出版社,2019.