Journal of Computer Applications ISSN 1001-9081 2016-【-10
计算机应用,2016,【(【): 【-【 CODEN JYIIDU http://www.joca.cn

文章编号:1001-9081(2016)【-0000-00 doi:10.11772/j.issn.1001-9081.2016.【.0000

一种 APT 攻击分层表示模型

谭韧[1]，殷肖川[1*]，廉哲[1]，陈玉鑫[1]

(1.空军工程大学 信息与导航学院，陕西 西安 710077)

(*通信作者电子邮箱 redstorm@live.cn)

摘 要: 针对攻击链模型攻击阶段划分过细且无法表示攻击手段的问题，提出了一种 APT 攻击分层表示模型（APT-HARM）。通过总结分析大量公开的 APT 事件报告和参考 APT 攻击链模型与分层攻击表示模型（HARM），将 APT 攻击分为攻击链和攻击树上下两层，并将其形式化定义。首先将 APT 攻击分为由侦察、渗透、行动和撤出四个阶段组成的攻击链，并研究了各阶段特点；然后研究各阶段中采取的攻击手段，并依据其逻辑关系组成攻击树。APT 攻击按照攻击链分阶段依次进行，各阶段按照攻击树流程依次执行。案例分析表明，本模型相较攻击链模型具有粒度划分合理，攻击描述完备准确的优点。APT-HARM 形式化地定义了 APT 攻击，为 APT 攻击的预测和防范提供了一种思路。

关键词: 高级可持续性威胁；攻击链；攻击树；分层攻击表示模型

中图分类号:TP309 **文献标志码: A**

A Hierarchical Representation Model of APT Attack

TAN Ren[1,2], YIN Xiaochuan[1*], LIAN Zhe[2], CHEN Yuxin[2]

(1. Information and Navigation College, Air Force Engineering University, Xi'an 710077, China)

Abstract: The attack chain model was too small-grained in representing APT attack phase and cannot indicate the attack method. To solve this problem, a hierarchical attack representation model of APT attack (APT-HARM) was proposed. By analyzing the APT event report and referring to the APT attack chain model and the hierarchical attack representation model (HARM), the APT attack was divided into two layers, the upper layer attack chain and the lower layer attack tree. Firstly, the APT attack was divided into four phases of reconnaissance, infiltration, operation and exfiltration and the characteristics of each stage were studied. Then, the attacking method in each stage was analyzed, and the attack tree was composed according to its logical relations. APT attacks were carried out in stages according to the attack chain, and the attack of each stage was performed in accordance with the attack tree. The case study shows that the model has the advantages of reasonable granularity classification and better attack description compared to the attack chain model. APT-HARM formally defines the APT attack, which provides an idea for the prediction and prevention of APT attacks.

Keywords: Advanced persistent threat(APT); attack chain; attack tree; hierarchical attack representation model(HARM)

0 引言

现代社会的运转已经愈发离不开互联网，各类信息及工业控制系统，例如金融、交通、电力系统等，都需要互联网支撑其正常运转。而高级可持续性威胁（Advanced Persistent Threat，APT）[1]攻击的出现，给网络空间安全提出了一个棘手的挑战。APT 的类型可分为两种：其一是窃密型，即入侵目标系统后窃取知识产权及其他信息，例如 2011 年 10 月发生的 Duqu APT 攻击[2]；其二是破坏型，即入侵目标系统后破坏数据，软件甚至是硬件设施，例如 2010 年发生的 Stuxnet APT 攻击[3]。无论是窃密型还是破坏型 APT 攻击都能给运行在互联网上的信息系统造成严重危害。

Symantec 和 ANRC 相继发布白皮书指出[4,5]，APT 攻击目标极为明确，具有很强的反侦察能力，同时拥有高级而复杂的攻击工具与手段，一般使用一个或多个 0day 漏洞[6]实施攻击，因此防病毒软件很难检测并从系统中清除恶意代码。而 APT 攻击往往持续几个月甚至几年，可疑流量基本隐藏在正常流量当中，这给传统的入侵防御系统提出了极大的挑战。因此，为了增强对 APT 攻击的防御能力，有必要对 APT 攻

收稿日期: 2016-00-00; **修回日期**:2016-00-00。**基金项目**: 国家自然科学基金资助项目（61402510）；陕西省工业科技攻关项目（2016GY-087）

作者简介: 谭韧(1993—)，男，湖南娄底人，硕士研究生， CCF 学生会员(会员号 73493G)，主要研究方向：网络与信息安全；殷肖川(1961—)，男，湖北武汉人，硕士生导师，博士，主要研究方向：网络与信息安全，数字水印技术；廉哲(1993—) 男，山西运城人，硕士研究生，主要研究方向：网络与信息安全；陈玉鑫(1993—) 男，甘肃兰州人，硕士研究生，主要研究方向：网络与信息安全。

击的攻击阶段，攻击目标和攻击方法展开研究，建立形式化模型，从而有针对性地防范 APT 攻击。

Hutchins 等人[7]针对常规的网络防御手段（例如入侵检测系统和防病毒系统）难以防范手段复杂多样的 APT 攻击的问题，以阻止 APT 攻击为目标，通过对各阶段攻击特点的分析，最先提出了 APT 攻击 7 阶段攻击链模型（Intrusion Kill Chain，IKC）。第一阶段是侦察，进行信息搜集和目标选择；第二阶段是武器化，进行 APT 恶意程序制作；第三阶段是传播，将恶意程序释放到目标系统；第四阶段是漏洞利用，运用操作系统和应用程序的漏洞触发恶意程序；第五阶段是安装，即安装远程控制软件或者后门程序；第六阶段是指控，即恶意程序与外部攻击者建立指控通路，使得攻击者能够控制内部网络；最后一个阶段是行动与目标，即实施破坏或是窃取信息。文中指出，攻击链中各阶段均按照顺序执行，任一阶段被阻止都会使得攻击失败。IKC 模型使用攻击链来同时描述 APT 攻击的各个阶段以及其攻击手段，这样带来了从攻击阶段考虑表示粒度过细，而从攻击手段考虑表示粒度过粗的问题。Symantec 公司先后在文献[4]和文献[8]中提到了 APT 攻击链，前者依次包含入侵，发现，获取和渗出四个阶段，后者在入侵阶段之前加入了侦察阶段。该攻击链模型较好的说明了 APT 攻击各阶段特点及典型的攻击方法，但是没有对 APT 攻击进行形式化描述，难以对其进行有效运用。Li 等人[9]更进一步地提出了 APT 攻击 4 阶段攻击模型，分别是准备阶段，进入阶段，驻留阶段和收割阶段。准备阶段主要完成信息搜集和恶意软件开发；进入阶段主要完成社会工程学攻击和直接攻击；驻留阶段完成内网信息搜集、提升权限、远程控制和横向移动[10]；收割阶段主要完成信息回传和痕迹清理工作。文中也介绍了最新的社会工程学方法，如鱼叉式网络钓鱼[11]和水坑攻击[12]。但是该模型只分析了窃密型 APT 攻击而没有对破坏型 APT 攻击进行分析，也没有对 APT 攻击进行形式化定义。业界提出的渗透测试标准 PTES[13]以攻击者的视角详细说明了一次网络攻击的攻击流程，包括情报搜集，威胁建模，漏洞分析，渗透攻击和后渗透攻击等。在每一个流程阶段都有相应的攻击要素和攻击方法，这对针对性防范 APT 攻击提供了参考。廉哲等[14]针对 APT 防御态势获取问题，使用软件定义网络（Software Defined Networking，SDN）技术架设虚拟蜜网。通过诱骗诱骗攻击者对网内节点进行攻击，可记录攻击行为并加以分析。

从 Hutchins 等人提出 APT 攻击链的 7 个阶段开始，IKC 模型便广泛运用在 APT 攻击的表示中。该模型能够十分清晰的描述 APT 攻击进行的流程以及各个阶段的主要特点，但是没有对各阶段的主要攻击手段进行详细分析，同时也没有对模型进行明确的形式化描述。而 APT 攻击与传统的网络攻击有着较多不同，各阶段攻击手段之间存在着较为复杂的组合关系，单纯使用攻击链模型难以对其进行描述。针对上述问题，本文通过总结大量公开的 APT 攻击分析报告，结合 HARM 模型[15]提出一种 APT 攻击分层表示模型 APT-HARM(APT Hierarchical Attack Representation Model)，给出了 APT 攻击的形式化定义，并利用相关 APT 攻击案例对模型进行了对比说明。

1 APT 攻击表示模型

本文形式化的定义了两层的 APT 攻击分层表示模型 APT-HARM。分别为上层的攻击链和下层的攻击树。

1.1 相关定义

定义 1 APT-HARM 由三元组 $L=(AC,AT,M)$ 表示。AC 指模型上层的攻击链，ac_i 指攻击链中某一阶段。AT 指模型下层的攻击树，at_i 表示某一攻击阶段对应的攻击树。$M=AC\mapsto AT$ 指 ac_i 到 at_i 的映射关系。

定义 2 攻击链 AC 位于 APT-HARM 的上层，由有向图 $C=(S,E)$ 表示。其中 S 是攻击链中 ac_i 的有限集；$E=\{(ac_i,ac_j,O_i)\}$，表示 ac_i 阶段完成目标 O_i 后可以迁移到 ac_j 阶段。

定义 3 攻击树 AT 位于 APT-HARM 的下层，由三元组 $T=(M,W,G)$ 表示。其中 M 表示可能采取的攻击手段或攻击子树的有限集，m_i 表示集中元素；W 指以 $\{(children,gate)\}$ 形式表示的二元组，其中 $children$ 表示当前子树中的 $\{m_i\}$，$gate\in\{AND\text{-}gate,OR\text{-}gate\}$；$G$ 为当前攻击树的目标，整棵树的目标是完成 AC 中的攻击目标 O。

定义 4 原子攻击是指 APT 攻击中不可再分的攻击形态。一种攻击手段只可能是或不是原子攻击，非原子攻击由原子攻击组成。

1.2 攻击链

本文提出了以侦察（Reconnaissance）、渗透（Infiltration）、行动（Operation）和撤出（Exfiltration）的 4 攻击阶段攻击链 RIOE。

1.2.1 侦查阶段

侦察阶段 ac_1 主要完成对攻击目标的信息搜集工作的目标 O_1。手段主要包括主动信息侦察、被动信息侦察和半被动信息侦察。在主动信息侦察中，攻击者要主动连接目标进行侦察，其主要的行为特点是扫描（Scanning），这种侦察方式能够获取到第一手且准确的信息，但由于主动信息侦察可能会被目标系统的网络防护设备发现，因此较少运用。在被动信息侦察中，攻击者不会发送任何流量给目标，只使用公开的第三方信息，这种侦察方式足够隐蔽，但是通过第三方获取到的信息可能过时甚至不正确。尽管如此，由于不会被目标系统所发现，被动信息侦察往往是 APT 攻击者的首选。

半被动信息侦察介于主动信息侦察和被动信息侦察之间，其将侦察行为尽量伪装成正常的网络流量和网络行为，目标系统可能会探测到侦查行为，但是无法对其进行溯源。

1.2.2 渗透阶段

渗透阶段 ac_2 主要完成对攻击目标进行渗透的目标 O_2。主要手段包括社会工程学攻击、水坑攻击、接触式攻击和漏洞攻击。社会工程学攻击[16]是一种通过社交网络或是其他途径获取目标敏感信息，随后利用这些信息进行进一步渗透的攻击方式。这种渗透方式利用了人性弱点，十分隐蔽，且难以被安全系统所察觉，攻击成功率较高。水坑攻击是在一种较为特殊的社会工程学方法，因此单独将其提出，主要手段是通过了解目标人员经常访问的网站，然后将其攻陷并植入恶意代码，当目标人员再次访问该网站时就会触发网页中的恶意代码，执行攻击者的指令。这样既不会直接发送攻击流量避免被溯源，也可以提高攻击的成功率和准确率。接触式攻击即采用非技术手段接触目标系统（例如直接插入 U 盘），植入 APT 病毒，这种方式成本代价较高，但是特异性和成功率非常高。漏洞攻击是较为底层的攻击方式，除了通过社会工程学手段直接获取目标系统管理权限外，几乎所有的其他攻击手段都要通过漏洞攻击加以实施。在实际的 APT 攻击中大量使用被称为 0day 漏洞[17]的当前未知漏洞，从而突破现有的安全防护体系获得系统控制权。

1.2.3 行动阶段

行动阶段 ac_3 主要完成在获取目标系统控制权后对攻击目标进行信息搜集或实施破坏的目标 O_3。主要手段包括建立指挥控制、控制持久化、信息窃取、实施破坏和横向移动。为了长时间在目标系统内行动，攻击者会用尽一切手段保持自身的隐蔽性。建立指挥控制（Command & Control，C2）通常是攻击者获取目标系统控制权后的第一个行动。通过隐蔽和加密信道，例如通过洋葱网络（The Onion Router，TOR）进行通信，或是包装成正常数据通信的信道对目标系统内植入的病毒进行指挥控制通信。控制持久化的目的是为了了解目标系统的硬件、软件和网络环境和寻找相应漏洞，有针对性地投送远程控制木马和后门等，以之对系统进行长期控制。信息窃取和实施破坏是整个 APT 攻击的核心目标。在获取系统控制权限、建立指挥控制链路、进行环境检查并上传相关工具后，攻击者开始依据最开始设定的目标进行信息窃取或是破坏活动。横向移动可以理解为渗透扩大化，即以已攻陷或是通过已攻陷的系统对同一网络中的其他系统进行渗透。对于攻击者而言攻击链又回到了渗透阶段。在真实的 APT 攻击中，攻击者往往不能直接获取到所需要的系统管理权限，需要逐步对核心系统进行渗透攻击。

1.2.4 撤出阶段

撤出阶段 ac_4 主要完成在预定行动完成后执行数据回传和痕迹清理的目标 O_4。主要手段包括回传敏感数据和删除日志记录。确定回传路径是回传敏感数据之前的必要操作，通常攻击者会选择与指控信道不同的路径进行信息回传，通过隐蔽和加密信道或是包装成正常数据通信进行数据回传。在数据回传时，攻击者需要确定控制链是否能够覆盖回传路径。由于过大的外泄流量会导致目标系统的察觉，因此有必要对回传的信息流量进行稀释，使其隐藏在常规的通信流量中，这使得要获得完整的数据需要相当长的时间，而文献[4]指出，APT 攻击的平均时间为 145 天，而最长可达 660 天，因此攻击者有足够时间获取到完整信息。在完成信息回传的同时，攻击者也要对攻击痕迹进行清理，防止被溯源。然而攻击者很难只清除自身活动的日志，特别是日志数量较多且存在备份的条件下。因此攻击者一般将攻击伪装成正常行为躲避日志审查，在必要时将删除所有日志。

1.2.5 形式化表示

攻击链 AC 由有向图 $C=(S,E)$ 表示。其中 $S=\{ac_1,ac_2,ac_3,ac_4\}$，$ac_1$ 至 ac_4 分别代表侦查阶段、渗透阶段、行动阶段和撤出阶段；$E=\{(ac_1,ac_2,O_1),(ac_2,ac_3,O_2),(ac_3,ac_2,O_3),(ac_3,ac_4,O_3)\}$，其中 (ac_3,ac_2,O_3) 代表横向移动。其图形表示如图 1 所示。

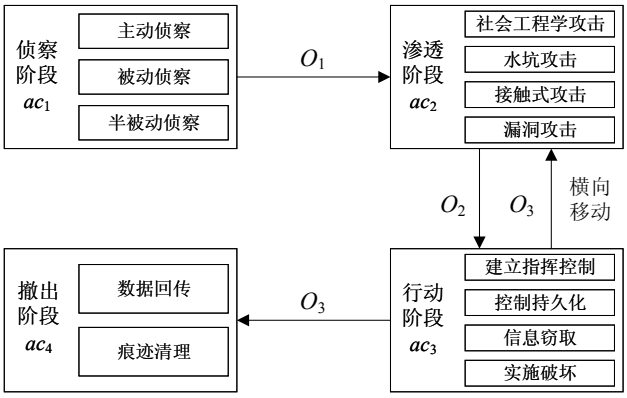

图 1 攻击链的图形化表示

Fig.1 Graphical representation of the attack chain

1.3 攻击树

攻击链中每一阶段都有其对应的完成各阶段目标的攻击树。前述各阶段的攻击手段均由对应的原子攻击组成。

1.3.1 侦察攻击树

侦察攻击树由主动信息侦察子树、被动信息侦察子树和半被动信息侦察子树组成，分别记为 m_{r1}，m_{r2} 和 m_{r3}。表 1 中 at_1 列出了侦察攻击树中包含的攻击方式。

在主动信息侦察中包含端口扫描、操作系统扫描、漏洞扫描和网络拓扑探查 4 种。被动信息侦察种包含 WhoIS 查询

和搜索引擎查询，著名的 Google Hacking 就属于搜索引擎查询。半被动信息侦察包括网络爬虫侦察和社交网络侦察。

1.3.2 渗透攻击树

渗透攻击树由社会工程学子树、水坑攻击子树、接触式攻击子树和漏洞攻击子树组成，分别记为 m_{i1}， m_{i2}， m_{i3} 和 m_{i4}。表 1 中 at_2 列出了渗透攻击树中包含的攻击方式。

社会工程学攻击包括鱼叉式网络钓鱼（Spear phishing）、网页钓鱼和社会工程学字典攻击等。在 APT 攻击中的鱼叉式网络钓鱼与传统意义上的钓鱼攻击不同，其前期收集了目标用户的相关社会信息，包括但不限于姓名，工作单位，职务等，大部分的垃圾邮件过滤器都难以对其进行有效防范，而依靠制定使用规定和用户培训也没有达到杜绝鱼叉式网络钓鱼的作用[18]，因此这是攻击者进行渗透的重要手段。水坑攻击包括注入攻击、跨站脚本攻击（Cross-Site Scripting，XSS）和跨站请求伪造（Cross-Site Request Forgery，CSRF）。接触式攻击包括移动存储设备接触和其他接触方式。漏洞攻击包括硬件漏洞攻击、操作系统漏洞攻击和应用系统漏洞攻击。无论是社会工程学攻击，水坑攻击还是接触式攻击，为了使得渗透行为不被目标防御系统察觉，最终都要使用漏洞攻击。从防御者的角度看，如何减少可被攻击者利用的漏洞成为防御 APT 攻击的关键问题之一。

1.3.3 行动攻击树

行动攻击树由建立指挥控制子树、控制持久化子树、信息窃取子树、实施破坏子树组成，分别记为 m_{a1}， m_{a2}， m_{a3} 和 m_{a4}。表 1 中 at_3 列出了行动攻击树中包含的攻击方式。

建立指挥控制主要涉及到加密通信和隐蔽通信，加密通信包括使用 SSL/TLS 和自定义的加密协议进行通信；隐蔽通信包括利用 TCP/IP 协议的未定义部分和伪装成正常协议的通信形式。控制持久化包括放置后门，放置木马和内存驻留。内存驻留是 APT 木马的高级形式，即不存在磁盘上的数据文件，一直驻留在系统内存中，因此难以发现与清除。信息窃取包括硬件信息搜集，操作系统信息搜集，应用程序信息搜集和用户信息搜集。实施破坏包括破坏硬件和损毁数据。

横向移动将部分或整个攻击流重定向到了渗透阶段，利用目前被攻陷的系统作为跳板或通路对更深层的系统进行渗透，直至完成预定目标。

1.3.4 撤出攻击树

撤出攻击树由执行数据回传子树和删除日志记录子树组成，分别记为 m_{e1} 和 m_{e2}。表 1 中 at_4 列出了撤出攻击树中包含的攻击方式。

执行数据回传主要涉及到确定回传路径，加密通信和隐蔽通信。而后两者在行动阶段中也起着关键作用，因此防御方如果能够阻断其进行加密和隐蔽通信则能够有效切断 APT 攻击链。删除日志记录包括设备日志销毁，操作系统日志销毁和应用系统日志销毁。

表 1 攻击树详细信息

Tab.1 Detailed information of the attack tree

攻击树	标记	描述	父节点	是否原子
at_1	m_{r1}	主动信息侦察	O_1	否
	m_{r2}	被动信息侦察	O_1	否
	m_{r3}	半被动信息侦察	O_1	否
	m_{x1}	端口扫描	m_{r1}	是
	m_{x2}	操作系统扫描	m_{r1}	是
	m_{x3}	漏洞扫描	m_{r1}	是
	m_{x4}	网络拓扑探查	m_{r1}	是
	m_{p1}	WhoIS 查询	m_{r2}	是
	m_{p2}	搜索引擎查询	m_{r2}	是
	m_{m1}	网络爬虫侦察	m_{r3}	是
	m_{m2}	社交网络侦察	m_{r3}	是
at_2	m_{i1}	社会工程学攻击	O_2	否
	m_{i2}	水坑攻击	O_2	否
	m_{i3}	接触式攻击	O_2	否
	m_{i4}	漏洞攻击	O_2	否
	m_{s1}	鱼叉式网络钓鱼	m_{i1}	是
	m_{s2}	网页钓鱼	m_{i1}	是
	m_{s3}	社工字典攻击	m_{i1}	是
	m_{w1}	注入攻击	m_{i2}	是
	m_{w2}	跨站脚本攻击	m_{i2}	是
	m_{w3}	跨站请求伪造	m_{i2}	是
	m_{c1}	移动存储设备	m_{i3}	是
	m_{c2}	其他接触方式	m_{i3}	是
	m_{v1}	硬件漏洞攻击	m_{i4}	是
	m_{v2}	操作系统漏洞攻击	m_{i4}	是
	m_{v3}	应用系统漏洞攻击	m_{i4}	是
at_3	m_{a1}	建立指挥控制	O_3	否
	m_{a2}	控制持久化	O_3	否
	m_{a3}	信息窃取	O_3	否
	m_{a4}	实施破坏	O_3	否
	m_{h1}	加密通信	m_{a1}, m_{e1}	是
	m_{h2}	隐蔽通信	m_{a1}, m_{e1}	是
	m_{t1}	提升权限	m_{a2}	是
	m_{t2}	放置后门	m_{a2}	是
	m_{t3}	放置木马	m_{a2}	是
	m_{t4}	内存驻留	m_{a2}	是
	m_{o1}	硬件信息搜集	m_{a3}	是
	m_{o2}	操作系统信息搜集	m_{a3}	是
	m_{o3}	应用程序信息搜集	m_{a3}	是
	m_{o4}	用户信息搜集	m_{a3}	是
	m_{d1}	破坏硬件	m_{a4}	是
	m_{d2}	损毁数据	m_{a4}	是
at_4	m_{e1}	执行数据回传	O_4	否
	m_{e2}	删除日志记录	O_4	否

	m_{b1}	确定回传路径	m_{e1}	是
	m_{k1}	设备日志销毁	m_{e2}	是
	m_{k2}	操作系统日志销毁	m_{e2}	是
	m_{k3}	应用系统日志销毁	m_{e2}	是

1.3.5 形式化表示

以行动攻击树为例对攻击树形式化定义进行说明。其余各阶段攻击树的表示与之类似，不再赘述。

行动攻击树以 $T=(M,W,G)$ 表示，其中 $M=\{m_{a1},m_{a2},m_{a3},m_{a4}\}$，$W=\{(\{m_{a1},m_{a2}\},AND\text{-}gate,O_3),(\{m_{a3},m_{a4}\},OR\text{-}gate,O_3)\}$，$G=O_3$。对于建立指挥控制子树 T_{a1}^m 而言，$M=\{m_{k1},m_{k2}\}$，$W=(\{m_{k1},m_{k2}\},AND\text{-}gate,m_{a1})$，$G=m_{a1}$。对于控制持久化子树 T_{a2}^m 而言，$M=\{m_{t1},m_{t2},m_{t3},m_{t4}\}$，$W=(\{m_{t1},m_{t2},m_{t3},m_{t4}\},OR\text{-}gate,m_{a2})$，$G=m_{a2}$。对于信息窃取子树 T_{a3}^m 而言，$M=\{m_{o1},m_{o2},m_{o3},m_{o4}\}$，$W=(\{m_{o1},m_{o2},m_{o3},m_{o4}\},OR\text{-}gate,m_{a3})$，$G=m_{a3}$。对于实施破坏子树 T_{a4}^m 而言，$M=\{m_{d1},m_{d2}\}$，$W=(\{m_{d1},m_{d2}\},OR\text{-}gate,m_{a4})$，$G=m_{a4}$。图形表示如图 2 所示。

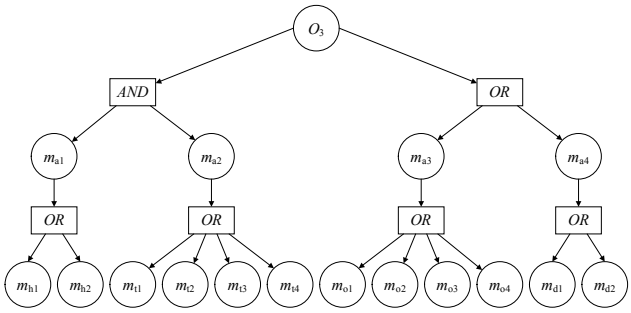

图 2 行动攻击树的图形表示

Fig.2 Graphical representation of the operation attack tree

1.4 **形式化表示**

APT-HARM 三元组 $L=(AC,AT,M)$，$AC=\{ac_1,ac_2,ac_3,ac_4\}$，$AT=\{at_1,at_2,at_3,at_4\}$，$M=\{ac_1\mapsto at_1,ac_2\mapsto at_2,ac_3\mapsto at_3,ac_4\mapsto at_4\}$。其中 AC 在 1.2.5 节中进行了说明，AT 在 1.3.5 节中进行了说明。

2 典型 APT 案例分析

Duqu 2.0 攻击[19]和夜龙（Night Dragon）攻击[20]是较为典型的 APT 攻击，前者针对世界领先信息安全厂商卡巴斯基实施信息窃取，后者针对欧美主要能源公司实施信息窃取。本节以这两个典型案例出发，对 APT-HARM 模型与 IKC 模型进行对比分析。

2.1 Duqu 2.0 攻击

Duqu 2.0 攻击链包含有 RIOE 的全部四个阶段，即侦查阶段，渗透阶段，行动阶段和撤出阶段。

在侦察阶段，攻击者至少掌握了目标的社会关系（实验室员工），电子邮件地址，计算机操作系统及其漏洞信息（0day 漏洞），初步拓扑信息。因此，攻击者使用了主动信息侦察、被动信息侦察和半被动信息侦察。其中使用了操作系统扫描，漏洞扫描，网络拓扑探查，WhoIS 查询和社交网络侦察等。

在渗透阶段，攻击者采用了极其具有针对性的电子邮件钓鱼，利用邮件将带有攻击载荷的 word 文档发送给目标，诱骗目标打开该文档，利用 CVE-2014-4148 漏洞获取系统控制权。因此，攻击者使用了社会工程学攻击和漏洞攻击。其中使用了鱼叉式网路钓鱼和操作系统漏洞攻击等。

在行动阶段，攻击者首先攻击者利用 CVE-2014-6324 和 CVE-2015-2360 漏洞将自身权限提升至管理员级别，随后利用被感染的计算机作为跳板攻击域内其他计算机，同时使用 MSI 安装包释放支持 C2 控制（182.253.220.29 和 186.226.56.103）的远程后门程序。使用正常的 SSL 和 HTTP 协议进行通信，同时使用图片信息隐藏技术进行通信。Duqu 2.0 使用的代码驻留方式十分特别，绝大部分代码运行在内存中，这样就很难发现磁盘上的异常。针对大规模断电导致内存信息丢失的问题，Duqu 2.0 在少数直连外部网络的计算机中驻留了支持远程桌面的后门程序，一旦发生载荷丢失问题可以立即重新安装。Duqu 2.0 可以看作是一个攻击平台，其通过不同的载荷实现不同的功能。在卡巴斯基实验室的报告中共描述了 5 种载荷，100 多种载荷插件以实现不同的功能，主要可以分为横向移动和信息窃取两类。就后者而言，其主要搜集 USB 设备、DHCP 及路由设备、已连接的打印机、网络适配器设置、防火墙策略等硬件信息；搜集运行进程列表、活跃终端会话、所有网络共享、安装的程序、域管理员 SID 及密码 HASH 等操作系统信息；搜集 POP3 密码、VNC 密码，数据库实例信息，PuTTY 主机密钥及会话等应用系统信息。因此，攻击者建立了指挥控制，使用了控制持久化技术和进行了信息窃取。其中使用了行动攻击树中除了破坏硬件和损毁数据的所有手段。

在撤出阶段，攻击者执行了数据回传和删除日志记录。在数据回传过程中，攻击者映射了内部网络的拓扑结构，突破了卡巴斯基互联网代理服务器，通过 Windows 管道，服务器信息通信（Server Message Block，SMB）等通过自定义的私有加密协议和与行动阶段类似的通信方式进行数据回传。同时，为了擦除攻击痕迹，攻击者删除了所有与攻击有关的日志信息，以至于卡巴斯基只发现了初始攻击来自于亚太地区某个员工的钓鱼邮件却无法发现攻击来源。因此，攻击者

执行了撤出攻击树所有的攻击手段。表 2 对 APT-HARM 模型与 IKC 模型对 Duqu 2.0 攻击的表示进行了对比。

表 2 两种模型对 Duqu 2.0 APT 攻击表示的比较

Tab.2 Comparison between APT-HARM and IKC in the representation of Duqu 2.0 APT attack

阶段	攻击树	攻击子树	攻击手段	详细信息	IKC 阶段
ac_1	at_1	m_{r1}	m_{x2}, m_{x3}, m_{x4}	Windows 系统；判明存在漏洞；初步网络信息	侦察阶段
		m_{r2}	m_{p1}, m_{p2}	服务器域名	武器化阶段
		m_{r3}	m_{m2}	电子邮件地址	
ac_2	at_2	m_{i1}	m_{s1}	精准钓鱼邮件	传播阶段
		m_{i4}	m_{v2}, m_{v3}	word 显示漏洞和 Windows 内核漏洞	漏洞利用阶段
ac_3	at_3	m_{a1}	m_{h1}, m_{h2}	SSL 等加密通信；图片隐藏信息通信	安装阶段
		m_{a2}	m_{t1}, m_{t2}, m_{t3}, m_{t4}	CVE-2014-6324，CVE-2015-2360 提权；特制攻击载荷	指挥控制阶段
		m_{a3}	m_{o1}, m_{o2}, m_{o3}, m_{o4}	攻击载荷搜集硬件，操作系统，应用程序和用户信息	行动和目标阶段
ac_4	at_4	m_{e1}	m_{b1}, m_{h1}, m_{h2}	寻找回传路径；SSL 等加密通信；图片隐藏信息通信	
		m_{e2}	m_{k1}, m_{k2}, m_{k3}	无法从日志寻找攻击源头	

2.2 夜龙攻击

Night Dragon 攻击的攻击链同样包括 RIOE 的全部四个阶段。

在侦查阶段，攻击者至少掌握了目标的社会关系（敏感计算机使用员工）以及其电子邮件地址，网页后台数据库软件信息以及其漏洞信息（SQL 注入漏洞），初步的拓扑信息。因此，攻击者使用了主动信息侦察，被动信息侦察以及半被动信息侦察。其中，使用了端口扫描，漏洞扫描，网络拓扑探查，搜索引擎查询，WhoIS 查询和社交网络侦察等攻击手段。

在渗透阶段，攻击者通过直接利用 SQL 注入漏洞进入管理后台获得网页服务器远程执行代码权限，随后发动了鱼叉式网络钓鱼攻击，利用邮件将远程控制工具（Remote Administration Tools，RAT）直接发送给目标人员，诱骗其运行程序使攻击者获得了目标人员操作系统的管理权限。因此，攻击者使用了社会工程学攻击和漏洞攻击，其中使用了鱼叉式网络钓鱼和应用系统漏洞攻击等。

在行动阶段，攻击者利用被攻陷的网页服务器和用户计算机作为跳板感染其他计算机，同时在被攻陷的网页服务器上建立 C2 服务器，并释放称为“zwShell”的 RAT 工具。攻击者通过虚拟专用网（Virtual Private Network，VPN）绕过了防火墙和 DMZ 直接进入内部网络进行横向移动扩大攻击，攻击者关闭了被攻陷的内网计算机上的代理设置，使得内网计算机能够直接与互联网进行通信。在控制持久化上，攻击者使用了动态 DNS 技术来保证被攻陷计算机总能通过特定域名访问到 C2 服务器，这些域名包括 is-a-chef.com，thruhere.net 等公开的动态 DNS 服务提供商，因此难以对攻击者进行溯源。攻击者使用正常的 HTTP 协议与被攻陷计算机进行数据传输，同时与 RAT 通信时使用了身份验证机制。zwShell 被设计为插件扩展式的多功能 RAT 工具，在迈克菲的报告中共提到了 7 种不同的攻击载荷，包括文件窃取，屏幕录制，命令执行，键盘监视等功能。因此，攻击者建立了指挥控制，使用了控制持久化技术和进行了信息窃取，同样使用了行动攻击树中除破坏硬件和损毁数据的所有手段。

在撤出阶段，攻击者执行了数据回传。在此过程中，攻击者通过 zwShell 直接将获取到的数据上传至 C2 服务器上，进而转发至攻击者手中，攻击者似乎对回传的数据没有使用任何加密手段，直接明文进行回传。在报告中没有明确提到攻击者删除日志记录的操作，因此攻击者执行了数据回传操作，其中进行了确定回传路径和隐蔽通信。表 3 对 APT-HARM 模型与 IKC 模型对夜龙攻击的表示进行了对比。

APT-HRAM 模型相较 IKC 模型有三点改进。一是合理划分了攻击阶段与攻击手段。IKC 模型使用攻击链统一描述 APT 攻击中的攻击阶段与攻击手段，这样就使得 APT 攻击的表示从攻击阶段而言粒度过细，而从攻击手段而言粒度过粗，本模型通过合并多余的攻击阶段和分别研究各阶段的攻击手段解决了这一问题。二是形式化地定义和表示了攻击阶段与

攻击手段的内部关系。通过将 APT 攻击的表示分为两层，既通过攻击链突出了 APT 攻击阶段递进关系，也通过攻击树表示了各攻击手段的内部逻辑关系以及攻击手段与攻击链中各攻击阶段的组合关系。三是补充了 IKC 的攻击阶段。在 IKC 模型中没有提到 APT 攻击的结束阶段，对 APT 攻击的表述不够完整，APT-HARM 模型提出了撤出阶段并分析了可能的攻击手段。

表 3 两种模型对夜龙 APT 攻击表示的比较

Tab.3 Comparison between APT-HARM and IKC in the representation of Night Dragon APT attack

阶段	攻击树	攻击子树	攻击手段	详细信息	IKC 阶段
ac_1	at_1	m_{r1}	m_{x1}, m_{x3}, m_{x4}	开放的服务端口；判明存在注入漏洞；初步网络信息	侦察阶段 武器化阶段
		m_{r2}	m_{p1}, m_{p2}	服务器域名	
		m_{r3}	m_{m2}	电子邮件地址	
ac_2	at_2	m_{i1}	m_{s1}	精准钓鱼邮件	传播阶段
		m_{i4}	m_{v3}	SQL 注入漏洞	漏洞利用阶段
ac_3	at_3	m_{a1}	m_{h1}, m_{h2}	C2 加密通信；HTML 隐藏信息通信	安装阶段 指挥控制阶段
		m_{a2}	m_{t2}, m_{t3}, m_{t4}	zwShell 远程 RAT；特制攻击载荷	
		m_{a3}	$m_{o1}, m_{o2}, m_{o3}, m_{o4}$	攻击载荷搜集硬件，操作系统，应用程序和用户信息	行动和目标阶段
ac_4	at_4	m_{e1}	m_{b1}, m_{h2}	寻找回传路径；HTML 隐藏信息通信	

3 结语

本文通过对大量公开的 APT 攻击事件的总结分析，结合 APT 攻击链模型和 HARM 模型，提出了 APT 攻击分层表示模型 APT-HARM，并利用典型 APT 攻击对本对模型与 LKC 模型进行了对比分析。APT-HARM 模型将 APT 攻击分为两层进行表示，上层为 4 个阶段组成的攻击链，下层为各阶段所可能采取攻击手段组成的攻击树。本模型相较于 IKC 模型具有结构划分合理，攻击描述完备准确的优点。APT 攻击依靠完整的攻击链，因此只要切断任意环节就可以阻止 APT 攻击。基于本模型可以对 APT 防御做进一步研究，如分析 APT 攻击中可能采取的关键攻击手段，有针对性地进行防护，从而阻止 APT 攻击。

参考文献

[1] BREWER R. Advanced persistent threats: minimising the damage[J]. Network Security, 2014, 2014(4): 5-9.

[2] BENCSÁTH B, PÉK G, BUTTYÁN L, et al. The cousins of stuxnet: Duqu, flame, and gauss[J]. Future Internet, 2012, 4(4): 971-1003.

[3] LANGNER R. Stuxnet: dissecting a cyberwarfare weapon[J]. IEEE Security & Privacy, 2011, 9(3): 49-51.

[4] SYMANTEC. Advanced persistent threats: a symantec perspective[R]. Mountain View, CA: Symantec Corporation, 2011.

[5] ALBULIWI R. ANRC Advanced Persistent Threat (APT) whitepaper[R]. San Antonio, Texas: ANRC, LLC, 2012.

[6] LAST D. Forecasting zero-day vulnerabilities[C]//Proceedings of the 11th Annual Cyber and Information Security Research Conference. [S.l.]: ACM, 2016: 13.

[7] HUTCHINS E M, CLOPPERT M J, AMIN R M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains[C], //Proceedings of the 6th International Conference on Information Warfare and Security. Washington: Curran Associates Inc. 2011: 113-125.

[8] DOHERTY S, BANERJEE D. Orchestrating Software Defined Networks (SDN) to disrupt the APT kill chain[R]. San Francisco, CA: RSA Conference, 2015.

[9] LI M, HUANG W, WANG Y, et al. The study of APT attack stage model[C]. 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS). [S.l.]: IEEE, 2016: 1-5.

[10] FAWAZ A, BOHARA A, CHEH C, et al. Lateral movement detection using distributed data fusion[C]. 2016 IEEE 35th Symposium on Reliable Distributed Systems (SRDS). [S.l.]: IEEE, 2016: 21-30.

[11] HONG J. The state of phishing attacks[J]. Communications of the ACM, 2012, 55(1): 74-81.

[12] O'GORMAN G, MCDONALD G. The elderwood project[R]. Mountain View, CA: Symantec Corporation, 2012.

[13] Penetration Testing Execution Standard. PTES Technical Guidelines[EB/OL]. [2017-3-9]. http://www.pentest-standard.org/index.php/Main_Page.

[14] 廉哲, 殷肖川, 谭韧, 等. 面向网络攻击态势的 SDN 虚拟蜜网研究[J]. 空军工程大学学报（自然科学版）, 2017, 18(3): 82-88.(LIAN Z, YIN X C, TAN R, et al. Research on SDN virtual honeynet for network attack situation[J]. Journal of Air Force Engineering University (Natural Science Edition), 2017, 18(3): 82-88.)

[15] HONG J B, KIM D S. Assessing the effectiveness of moving target defenses using security models[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(2): 163-177.

[16] NELSON J, LIN X, CHEN C, et al. Social engineering for security attacks[C]. Proceedings of the The 3rd Multidisciplinary International Social Networks Conference on SocialInformatics 2016, Data Science 2016. [S.l.]: ACM, 2016: 1-4.
[17] WANG L, JAJODIA S, SINGHAL A, et al. k-zero day safety: A network security metric for measuring the risk of unknown vulnerabilities[J]. IEEE Transactions on Dependable and Secure Computing, 2014, 11(1): 30-44.
[18] JUNGER M, MONTOYA L, OVERINK F J. Priming and warnings are not effective to prevent social engineering attacks[J]. Computers in Human Behavior, 2017, 66: 75-87.
[19] GLOBAL RESEARCH AND ANALYSIS TEAM. The Duqu 2.0 technical details[R]. Moscow: Kaspersky Lab, 2015.
[20] MCAFEE FOUNDSTONE PROFESSIONAL SERVICES AND MCAFEE LABS. Global Energy Cyberattacks:“Night Dragon”[R]. Santa Clara, CA: Mcafee Inc, 2011.

国家自然科学基金资助项目(61402510)；陕西省工业科技攻关项目(2016GY-087)

谭韧(1993—)，男，湖南娄底人，硕士研究生， CCF 学生会员，主要研究方向：网络与信息安全；殷肖川(1961—)，男，湖北武汉人，博士，硕士生导师，主要研究方向：网络与信息安全，数字水印技术；廉哲(1993—) 男，山西运城人，硕士研究生，主要研究方向：网络与信息安全；陈玉鑫(1993—)男，甘肃兰州人，硕士研究生，主要研究方向：网络与信息安全。

This work is partially supported by the the National Natural Science Foundation of China (61402510), the Industrial Research Project of Science and Technology Department of Shanxi Province (2016GY-087).

TAN Ren, born in 1993, M. S. candidate. His research interests are network and information security
YIN Xiaochuan, born in 1961, Ph. D, professor. His research includes network and information security, Digital Watermarking.
LIAN Zhe, born in 1993, M. S. candidate. His research interests are network and information security.
CHEN Yuxin, born in 1993, M. S. candidate. His research interests are network and information security.

本文矩阵、矢量（向量）变量符号说明:

无

本文内容的研究背景、基金项目介绍如下：

工作背景：通过对大量公开的 APT 报告进行分析，试图对 APT 攻击行为进行建模分析，寻找攻击中的关键步骤与所需的关键信息，使用技术和非技术手段阻断 APT 攻击链从而阻止 APT 攻击。

项目介绍：为了更好地节约成本和扩展业务功能，利用软件定义网络和网络功能虚拟化技术，充分利用现有普通交换设备通过软件定义化改造实现专用交换设备的功能。