基于树型结构的APT攻击预测方法

张小松[1]，牛伟纳[1]，杨国武[2]，卓中流[1]，吕凤毛[2]

(1. 电子科技大学网络空间安全研究中心 成都 611731；2. 电子科技大学大数据研究中心 成都 611731)

【摘要】近年来，高级持续性威胁已成为威胁网络安全的重要因素之一。然而APT攻击手段复杂多变，且具有极强的隐蔽能力，使得目前常用的基于特征匹配的边界防护技术显得力不从心。面对APT攻击检测防御难题，提出了一种基于树型结构的APT攻击预测方法。首先结合杀伤链模型构建原理，分析APT攻击阶段性特征，针对攻击目标构建窃密型APT攻击模型；然后，对海量日志记录进行关联分析形成攻击上下文，通过引入可信度和DS证据组合规则确定攻击事件，计算所有可能的攻击路径。实验结果表明，利用该方法设计的预测模型能够有效地对攻击目标进行预警，具有较好的扩展性和实用性。

关 键 词 高级持续性威胁； 攻击预测； 关联分析； 杀伤链

中图分类号 TP311 **文献标志码** A doi:10.3969/j.issn.1001-0548.2016.04.011

Method for APT Prediction Based on Tree Structure

ZHANG Xiao-song[1], NIU Wei-na[1], YANG Guo-wu[2], ZHUO Zhong-liu[1], and LÜ Feng-mao[2]

(1. Center for Cyber Security, University of Electronic Science and Technology of China Chengdu 611731;
2. Big Data Research Center, University of Electronic Science and Technology of China Chengdu 611731)

Abstract In recent years, advanced persistent threat (APT) has become one of the most important factors threatening cyber security. However, due to the complicated attacking method and strong conceal ability of APT, it is very hard to predict APT using the common boundary protection technique based on feature matching. To solve the problem of APT attack detection and defense, we propose an APT attacks prediction method based on tree structure. An APT exfiltration model of an attack target combing the kill chain model with stage characteristics is first constructed. And then the correlation analysis of massive logs is conducted to formulate attack events context, and the credibility ratio and DS evidence theory are introduced to determine true attack events. Finally, all possible attack paths are calculated. Experimental results show that our proposed method can predict APT attacks, and it can obtain good scalability and practicability.

Key words advanced persistent threat; attack prediction; correlation analysis; kill chain

国际上的网络攻击转向高级持续性威胁(advanced persistent threat, APT)[1]时日已久：2009年Google Gmail服务遭受30天APT攻击；2011年RSA私钥服务器被攻陷；2012年卡巴和Comodo公司源码被盗，以及超级病毒入侵中东多国造成重大核设施破坏等事件均和高级持续性网络攻击相关。

近几年，FireEye在InfoSec及Verizon等机构发表多份声明，披露APT攻击中的远控手段(GhostRat)。通过APT攻击溯源技术给出APT攻击受控于184个国家的命令控制(command&control, CC)服务器，得出增幅为2011年的1.2倍等结论。这一系列数据均表明国外对于APT攻击的研究与检测已经进入实战阶段[2-3]。我国也属于APT攻击受害国，但面向重要网络信息系统的专业防护服务能力和产业化程度相对较低，尚难以有效应对高级持续性威胁攻击，形势相当严峻。

APT攻击具有攻击行为特征难以提取、攻击渠道多元化、攻击空间不确定的特点。因此，APT攻击检测防御已成为业界公认的难题。而对APT攻击场景进行模型化分析，能够发现其实际开展过程中的相关规律，为检测防御APT[4-5]提供理论依据。

目前描述网络攻击的常用模型有攻击树模型[6]、攻击图[7]模型和基于Petri网[8]的攻击网络模型。攻击树模型具有可视化的层次结构，能够清晰描述APT攻击过程的阶段性特征。本文结合APT攻击中存在持续时间长、涉及领域广泛的特点，构建窃密型APT

收稿日期：2016－05－15
基金项目：国家自然科学基金项目(61572115, 61402080)；中国博士后科学基金(2014M562307)；四川省重大基础研究课题(2016JY0007)
作者简介：张小松(1968－)，男，长江学者特聘教授，主要从事数据安全、虚拟化与嵌入式平台安全、网络攻击检测与软件脆弱性方面的研究.

攻击树型模型，解决APT攻击建模难题；关联多源日志记录形成攻击上下文，结合证据相容性方法，确定攻击事件信任度；结合DS证据融合理论确定真实的攻击事件，最终利用APT攻击目标树型模型来预测未来可行的攻击路径。

1 相关介绍

1.1 杀伤链模型

最初用于作战过程中的杀伤链是指“发现-定位-跟踪-瞄准-攻击-评估”[9]这一完整流程。2011年3月Lock Martin公司的3位安全研究员在ICIW大会上首次提出IKC(intrusion kill chain)模型[10]。该模型从入侵检测的角度将攻击者的攻击过程分解为信息收集、组装、投放、利用、植入、命令&控制、持续攻击7个步骤。

1.2 APT攻击

APT攻击这一术语由USAF(united states air forces)[11]于2006年首次提出，从字面上解释就是一个有严密组织和充足资金支持的攻击团队不断尝试多种全方位、高隐蔽的攻击方法直到挖掘出关键信息或破坏关键设施。目前普遍采用美国国家标准协会(national institute of standards and technology, NIST)[12]在2011年给出的定义：具有高水平专业知识和丰富资源的攻击者通过使用多维攻击手段(如：网络、物理和欺骗)来达到特定目的(包括：窃密、阻碍重要任务实施和破坏基础设施)。

目前，APT攻击检测方法集中在从技术角度判断攻击行为是否是高级的、多重的、联合的以及定制化的。主流的APT攻击检测方法有恶意代码检测[13]、主机应用保护[6]、网络入侵检测[14]和大数据分析[15]，恶意代码检测产品通常部署在互联网入口点，可以在APT攻击的初始阶段对攻击进行检测、发现；网络入侵检测可以在网路层对APT攻击行为进行检测，如果攻击者通过跳板对内网进行渗透攻击，网络入侵检测系统可以进行预警、定位；主机应用保护可以防止APT攻击者将计算机中的敏感数据外传，可以有效降低攻击行为所造成的损失；大数据分析检测可以覆盖APT攻击的各个环节，已成为APT攻击检测防御的常用和有效手段。

2 APT攻击建模

树型结构不仅能够可视化展示APT攻击阶段，还能够预测攻击走向。所以，采用树型结构对APT攻击进行建模是切实可行的。

2.1 APT攻击阶段

虽然近年来曝光的APT攻击案例的具体攻击流程不同，但其在具体实施过程中具有阶段性[16]。结合具有较强普适性的IKC模型，通过对实际APT攻击事件的分析总结，将APT攻击过程划分为信息侦查、样本投放、初次入侵、对象操控、攻击收益、事后逃逸6个阶段，如图1所示。

1) 信息侦查：除了常用的主机勘测和漏洞扫描外，还使用大数据分析技术挖掘隐私信息和社会工程学收集相关信息。

2) 样本投放：通过邮件附件、网站和USB移动介质等途径将封装到程序或者客户端的病毒/木马投放到目标环境中。

3) 初次入侵：利用目标系统的漏洞执行恶意代码，进而获得目标主机或网络的非授权访问权限。

4) 对象操控：通过安装远程访问的木马或后门保持对目标系统的持续访问。

5) 攻击收益：窃取敏感信息或破坏目标系统的基础设施。

6) 事后逃逸：利用各种技术手段毁尸灭迹。

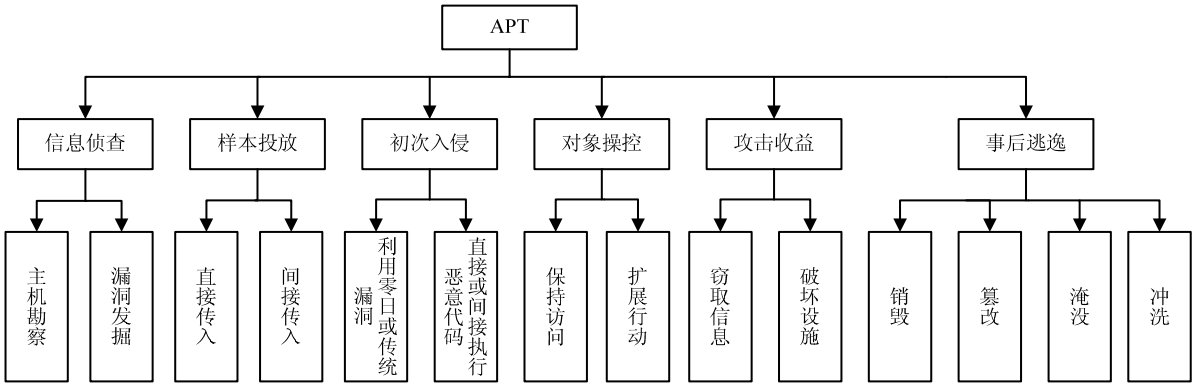

图1　APT攻击阶段

2.2 基于树型结构的窃密型APT攻击模型

基于杀伤链模型，结合APT攻击阶段的无后效性[17]，即下一阶段发生的事件只与上一阶段有关，构建针对目标节点的窃密型APT攻击树形模型，如图2所示。

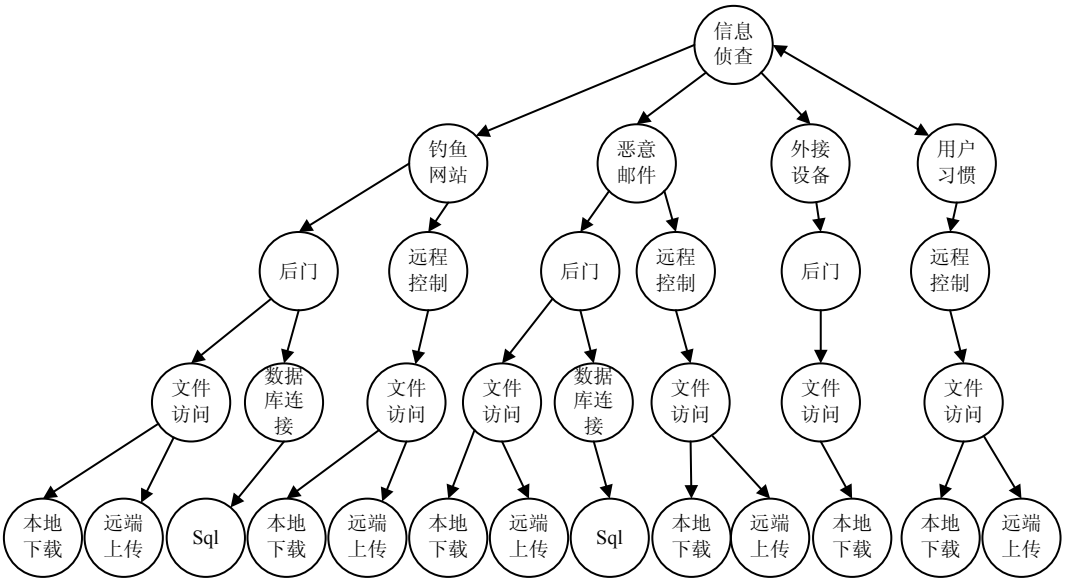

图2 基于树型结构的窃密型APT攻击模型

1) 信息侦查：攻击者通过对目标用户以及目标主机进行信息搜集，进而了解目标主机的系统环境和漏洞信息以及目标主机用户的行为习惯，便于设计下一步攻击的可行方案。APT攻击过程都会进行这一阶段，所以在这里不再进行细分。

2) 样本投放：可以分为直接传入和间接传入两种方式。其中，直接传入主要通过向目标发送含有恶意附件的电子邮件的方式实现。间接传入可以通过建立钓鱼网站使目标用户上当或通过含有恶意程序的U盘等设备使目标主机种马，或利用社会工程学手段，例如根据用户的使用习惯猜测用户的账号密码等。样本投放的具体方式由第一阶段搜集到的目标主机或目标用户信息的具体特点决定。

① 如果攻击者在信息侦查阶段发现目标用户经常利用搜索方式访问同一个网站却不了解网站的具体网址，则可以通过构建含有木马或其他恶意程序的钓鱼网站对用户进行攻击，当用户访问钓鱼网站时就可以在用户主机上植入恶意软件。

② 如果攻击者在信息侦查阶段发现用户经常向一些用户发送含有附件的邮件，则可以伪装成目标用户的朋友向其发送恶意邮件，该邮件中含有可执行的恶意程序的附件，当目标用户下载附件时便在目标主机上植入恶意软件。

③ 如果攻击者在信息侦查阶段发现用户在注册账号时喜欢使用同样的ID和密码，则可以使用该规律猜测用户的用户名和密码，当用户开启远程访问服务时，可以远程控制目标主机，并在目标主机上安装后门。

④ 如果攻击者在信息侦查阶段发现目标用户常使用外接设备传输数据，则可以选定目标用户的特定朋友作为跳板对目标主机进行攻击。首先攻击目标用户的朋友，然后在目标用户朋友的主机以及设备上安装恶意程序，当其朋友通过U盘等移动介质与目标主机进行通信时达到间接攻击目标主机的目的。

3) 初次入侵：经过样本投放阶段，攻击者便与目标用主机建立了通信信道，攻击者利用该通道可以在目标主机上安装后门或者远程控制目标主机。

① 通过钓鱼网站和恶意邮件的方式进行样本投放时，由于网页和附件等方式本身的限制，导致该方法不能直接嵌入过大且拥有复杂功能的木马，所以攻击者一般会选择先在目标主机上安装一个小型的恶意应用。该小应用一般具有两种功能，一是这个应用会在后台偷偷启动，然后连接到指定的主机下载下一步使用的恶意软件(此类应用会在后台启动并运行，然后窃取用户的资料)。二是打开目标主机的远程控制服务，攻击者利用该服务盗取用户的账户信息，进而实现远程控制目标主机的目的。假如目标主机的远程控制服务在信息侦查阶段就被发现是开启的，则攻击者可以直接远程登陆目标主

机对其实施远程控制。

② 样本投放阶段利用带有恶意程序的外接设备进行进一步攻击时，该恶意程序会在目标主机上运行。

4) 对象操控：通过初次入侵，攻击者已经在目标用户的电脑中安装了对应的恶意程序或者启动了远程控制，此时攻击者已经拥有了对目标主机中文件的访问权限。

① 攻击者可以利用安装后门的方式登录目标主机，获取相应权限并寻找需要的数据。

② 攻击者采用远程控制方式访问目标主机时，由于攻击者对目标主机的文件管理组织方式不了解，所以一般只能利用远程控制服务对文件系统进行遍历。

5) 窃取数据：攻击者在获取对目标主机控制权后，会查找敏感数据并对其进行窃取。根据数据存放方式的不同，常用的窃取途径分为以下两种：

① 当敏感数据存储在文件系统中时，经过上一阶段的操作已经找到了对应的文件存放处，此时便可以通过网络将数据传输到指定主机或者将数据拷贝到移动存储介质中还可以通过网络将无用数据或者有其他意图的数据写入到目标主机中。

② 如果敏感数据存储在数据库中，则攻击者可能使用远程控制方式运行指定的SQL语句将敏感数据盗走。

基于树型结构的APT攻击模型可以用$S(T, N_g)$表示，N_g表示攻击目标，在这里指存储在目标主机上的重要资料或资产；$T=\{N, B\}$，其中N是树中节点N_{ij}的集合，$i(i=1,2,3,4,5)$表示树中节点所处的层次，即APT攻击过程中使用的事件所在的攻击阶段，j是i层节点的索引。B表示树中有向边(N_{ij}, N_{mn})的集合，N_{mn}是N_{ij}下一阶段的节点，所以$m=i+1$。

3　APT攻击预测方法

Verizon机构发布的《Data Breach Investigations Report》[16]指出86%的已公开APT攻击被监控并存有记录，所以APT攻击者在攻击过程中会在不同的安全设备上留下蛛丝马迹，且基于大数据分析的APT攻击检测准确率较高，所以本文融合三层不同来源的日志记录，结合DS证据理论预测攻击路径，总体架构如图3所示。

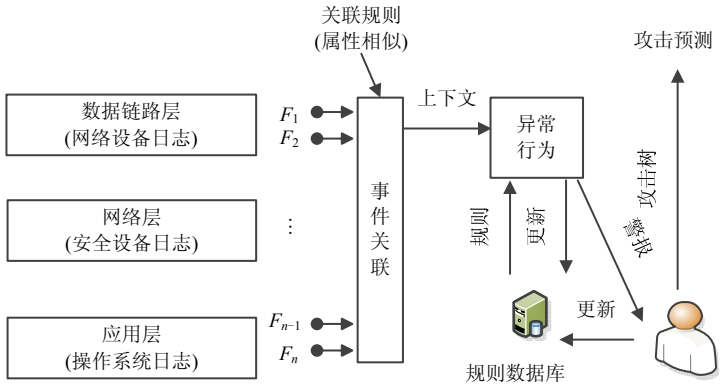

图3　APT预测框架

其中，$F_1,F_2,\cdots,F_n$为操作系统日志、安全设备日志、网络设备日志。其检测流程如下：

1) 利用APT目标档案(重要员工ID、数据库服务器IP、服务端口等)将收集到的日志记录按照属性相关性归整成上下文。

2) 使用检测算法处理上下文中的某段时间内(数小时、数周、数月甚至数年)整理的上下文，识别与目标相关的可能的攻击行为。

3) 基于当前攻击事件的信任度预测攻击者所有可行的攻击路径。

3.1　关联规则

$S_i=\{e_i^1, e_i^2, \cdots, e_i^{k_i}, \cdots\}, i=1,2,3,$ 表示APT预测框架中第i个来源中的所有日志记录，$e_i^j=(t, \mathrm{id}, a_1^j, a_2^j, \cdots, a_{mi}^j)$表示日志源$S_i$中第$j$个日志记录，$t$表示日志被记录的时间，id是标识符，$a_1^j, a_2^j, \cdots, a_{mi}^j$表示日志记录的属性，据此定义规则$r$即日志记录之间的关联函数为：

$$r(e_j^{k_i}, e_j^{k_j})=\begin{cases}1 & (F(a(e_i^{k_i}), a(e_j^{k_j})))=\mathrm{TRUE}\\ 0 & \text{其他}\end{cases}$$

式中，$a(e_i^{k_i})$表示日志记录$e_i^{k_i}$的属性；F表示日志记录的属性相同。

3.2　异常判断

上下文是由日志记录和APT目标档案数据根据关联规则直接提取的，它能将不同的日志记录相关

联，形式化为：$A=\{S_i, R, W, C, G\}$，其中S_i表示第i层安全设备收集到的与APT攻击目标G相关的日志记录集合，R表示上下文关联规则，W表示上下文有效的时间(数小时、数天、数月等)，C表示攻击可信度。

表1中所示的攻击轨迹是根据网络安全设备日志记录进行划分的，便于进行攻击上下文的匹配来确定当前目标环境所遭受的攻击类型，使得安全管理者有效预测所有可能的攻击路径。

表1 APT攻击及其含义

攻击轨迹	匹配规则
端口扫描	T时间内目标主机的N个端口收到请求
钓鱼网站	目标主机访问具有不同IP但网址相似的网站，且其目的IP不在本地DNS缓存中
恶意邮件	目标主机收到相似于其常用联系人邮箱发送的邮件，且该邮件含有附件
移动存储设备	目标主机连接外接存储介质，可执行程序在该外接设备上自动执行
后门安装	目标主机上安装程序，且该程序在未授权状态下执行
远程访问控制	目标主机开启远程访问服务
文件系统访问	T时间内目标主机的文件系统被有序遍历
数据库系统访问	目标主机的数据库访问服务开启，且T时间内数据项被有规律遍历

3.3 攻击路径预测

本文提出的攻击路径计算方法包括以下几个关键步骤：

1) 确定攻击目标，包括重要、敏感数据以及重要实体资产等，建立APT攻击目标源，集合$G=\{G_1, G_2, G_3, \cdots\}$表示攻击目标。

2) 针对目标节点建立基于树型结构的窃密性APT阶段模型：

① 对来自不同源的日志记录进行关联分析形成关联上下文；

② 将获取到的上下文与规则数据库进行匹配，发现攻击事件，即对应到树中的某个节点，且不同的日志记录设备对该攻击事件的可信度是不同的；m_i为第i层安全设备的信任度，u_j为第j个攻击事件，这里$m_i(u_j)$表示第i层日志记录设备对第j个攻击事件的信任度；

③ 将获取到的不同证据(即不同安全设备对攻击事件的可信度)进行融合计算，得到新的可信度，其中没有任何证据支持的节点(即没有任何日志记录和此事件相关)不进行计算。基于证据相容性方法的融合过程如下[19]：

用 $R_{i,j}=\dfrac{m_i(u_k)m_j(u_k)}{\dfrac{m_i(u_k)m_i(u_k)+m_j(u_k)m_j(u_k)}{2}}$ 计算证据之间的相容系数，进而获得安全设备i和j对攻击事件u_k的相容矩阵；

基于相容矩阵，使用 $D_i(u_k)=R_{i,j}(u_k), i,j=1,2,\cdots,n$ 计算攻击事件u_k的绝对相容度；

用 $m_i(u_i)\_\text{new}=\omega_i\ m_i(u_i)$ 更新安全设备i对攻击事件u_k的信任度，其中 $\omega_i(u_k)=\dfrac{D_i(u_k)}{n-1}$ 为攻击事件u_k的权重；

利用经典的DS证据融合理论计算各个攻击事件的信任度。

3) 计算所有可行攻击路径的可信度，并且根据后续时间窗内的日志记录对上一阶段的攻击过程进行修剪。

4 实验仿真

通过搭建网络环境模拟暗鼠行动的攻击流程：同时利用用户习惯和钓鱼网站的方式对目标主机进行攻击，且通过用户习惯进行攻击的过程没有取得成功。对多源日志记录进行关联分析，并与攻击规则进行匹配得到不同日志源对攻击事件的可信度，三层日志源对于第二阶段的四种攻击渠道的可信度如表2所示。

表2 三层日志源对四种攻击渠道的可信度

日志源	钓鱼网站	恶意邮件	外接设备	用户习惯
网络设备	0.7	0	0	0.3
安全设备	0.6	0	0	0.4
操作系统	0.5	0	0	0.5

模拟环境中，网络设备提供的攻击者采用钓鱼网站向目标发送恶意链接的攻击方式信任度为0.7，对攻击者使用社会工程学猜测目标用户的账户密码来实施攻击的信任度为0,3，其余为0，表示在当前情况下，没有证据证明目标主机被攻击者使用其他渠道进行攻击。因此，可以直接不考虑树的第二条分支树和第三条分支树，只需要计算钓鱼网站和用户习惯的最终的信任度。

然后，根据相容性定义计算所有通过钓鱼网站进行攻击的攻击事件和通过用户习惯进行攻击的攻击事件的相容性矩阵分别为$\boldsymbol{T}_1$和$\boldsymbol{T}_2$：

$$\boldsymbol{T}_1=\begin{pmatrix}1 & 0.988\,235 & 0.945\,946\\ 0.988\,235 & 1 & 0.983\,607\\ 0.945\,946 & 0.983\,607 & 1\end{pmatrix}$$

$$\boldsymbol{T}_2=\begin{pmatrix}1 & 0.96 & 0.882\,353\\ 0.96 & 1 & 0.975\,61\\ 0.882\,353 & 0.97\,561 & 1\end{pmatrix}$$

根据相容性矩阵计算日志源对攻击事件的新的信任度，得到钓鱼网站进行攻击的攻击事件和通过用户习惯进行攻击的攻击事件的新的可信度如表3所示。

表3　攻击事件的新的可信度

设备源	钓鱼网站	用户习惯	其他
m_1	0.676 963	0.276 353	0.046 684
m_2	0.591 553	0.387 122	0.021 325
m_3	0.482 388	0.464 491	0.053 121

每个攻击事件融合后的新的可信度如表4所示。

表4　攻击事件融合后的信任度

攻击事件	信任度
钓鱼网站	0.664 532
用户习惯	0.191 844
其他	0.143 624

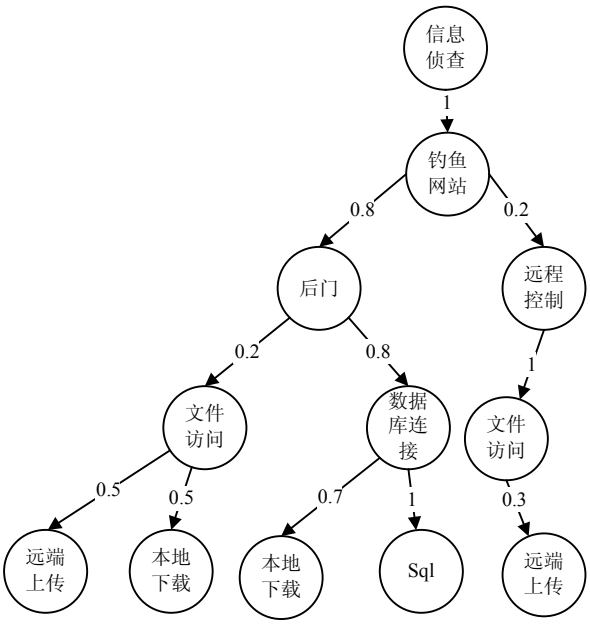

图4　攻击者可能采取的攻击路径

说明攻击者极有可能利用钓鱼网站向目标主机注入恶意软件。然后根据下一阶段的证据继续进行判断，发现有日志记录表明攻击者使用了远程控制手段与被攻击主机建立通信，所以可以判断出上一阶段使用的攻击途径是钓鱼网站，推测出攻击者可能采用用户习惯去猜测用户密码然而并没有成功。由此可知，攻击者可能采取的攻击路径如图4所示。也就是说，攻击者极有可能通过这些路径破坏攻击目标。在制定保护措施时，应该针对这些攻击方式重点采取防御措施。

5　结 束 语

本文通过杀伤链模型划分APT攻击过程，结合阶段内攻击事件的无后效特性，针对攻击目标主机构建基于树型结构的窃密型APT攻击模型。融合多源日志记录形成攻击上下文，映射归结为树中节点，结合基于权重的证据融合理论更新攻击树并计算出所有可行的攻击路径。与之前的方法相比，本文方法结合实际环境中日志源提供的证据间存在冲突与包容共存的情况，在不改变DS证据组合规则的前提下，引入证据相容性概念，通过关联日志记录获取的攻击事件可信度来更加客观地计算证据权重，并重新分配可信度，进而运用DS证据组合规则进行证据融合。实例证明，融合后的结论更加符合实际情况，进一步说明了本文提出的攻击路径预测方法具有可行性。

参 考 文 献

[1] ASK M, BONDARENKO P, REKDAL J E, et al. Advanced persistent threat (APT) beyond the hype[R]. Norway: Gjøvik University College, 2012.

[2]LI F, LAI A, DDL D. Evidence of advanced persistent threat: a case study of malware for political espionage[C]// Proceedings of the 2011 6th International Conference on Malicious and Unwanted Software (MALWARE). Fajardo: IEEE Computer Society, 2011: 102-109.

[3] CHEN P, DESMET L, HUYGENS C. A study on advanced persistent threats[C]//Communications and Multimedia Security. Berlin, Heidelberg: Springer, 2014: 63-72.

[4] TANKARD C. Advanced persistent threats and how to monitor and deter them[J]. Network Security, 2011(8): 16-19.

[5] COLE E. Advanced persistent threat: Understanding the danger and how to protect your organization[M]. Netherlands: Elsevier, 2012.

[6] GIURA P, WANG W. A context-based detection framework for advanced persistent threats[C]//Proceedings of the 2012 ASE International Conference on Cyber Security. Alexandria: IEEE Computer Society, 2012: 69-74.

[7] 牛伟, 戴卫国. APT攻击建模与安全防护技术研究[J]. 电子对抗, 2014(2): 34-38.
NIU Wei, DAI Wei-guo. Analysis on modeling and protection technique of APT attack[J]. Electronic Warfare, 2014(2): 34-38.

[8] ZHAO W, WANG P, ZHANG F. Extended petri net-based advanced persistent threat analysis model[C]//Proceedings of the 2013 International Conference on Computer Engineering and Network. Heidelberg: Springer, 2014: 1297-1305.

[9] 陈庄, 王国栋, 常俊杰. 基于杀伤链模型的工业控制系统信息安全分析[J]. 电子技术与软件工程, 2015(23): 206-208.
CHEN Zhuang, WANG Guo-dong, CHANG Jun-jie.

Information security analysis of industrial control system based on kill chain model[J]. Electronic Technology & Software Engineering, 2015(23): 206-208.
[10] 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.
[11] Websense. Advanced persistent threats and other advanced attacks[EB/OL]. [2016-02-21]. http://www.websense.com/assets/white-papers/whitepaper-websense-advanced-persistent-threats-and-other-advanced-attacks-en.pdf.
[12] GARY L, PATRICK D. Gallagher. Managing information security risk[R]. America: National Institute of Standards and Technology, 2011.
[13] LI F, LAI A, DDL D. Evidence of advanced persistent threat: a case study of malware for political espionage[C]// 2011 6th International Conference on Malicious and Unwanted Software (MALWARE). [S.l.]: IEEE Computer Society, 2011: 102-109.
[14] SIDDIQUI S, KHAN M S, FERENS K, et al. Detecting advanced persistent threats using fractal dimension based machine learning classification[C]//Proceedings of the 2016 ACM on International Workshop on Security And Privacy Analytics. [S.l.]: ACM, 2016: 64-69.
[15] GIURA P, WANG W. Using large scale distributed computing to unveil advanced persistent threats[J]. Science J, 2012, 1(3): 93-105.
[16] VRIES, J D, HOOGSTRAATEN H, BERG J V D, et al. Systems for detecting advanced persistent threats cybersecurity: a development roadmap using intelligent data analysis[C]//Procedings of the 2012 International Conference on Cyber Security. Washington, USA: IEEE Computer Society, 2012: 54-61.
[17] IOANNOU G, LOUVIERIS P, CLEWLEY N, et al. A markov multi-phase transferable belief model: an application for predicting data exfiltration APTs[C]//2013 16th International Conference on Information Fusion (FUSION). [S.l.]: IEEE, 2013: 842-849.

编 辑 蒋 晓

张小松(1968—)，教授，博士生导师、长江学者特聘教授。现为网络空间安全研究中心主任。主要从事大数据安全与应用、虚拟化与嵌入式平台安全、网络攻击检测与软件脆弱性等方面的研究，领导团队承担完成数十项军、民信息安全领域的国家和省部级课题，主持研制的网络和信息化平台在应用中取得重要的社会和经济效益。近年来分别获得2012国家科技进步二等奖，2013/2010四川省科技进步一等奖，2013电力行业信息化优秀成果一等奖，2008四川省科技进步二等奖。在CCF(中国计算机学会)推荐A类顶级学术期刊TSE、IEEE T RELIAB、FGCS等学术期刊上发表SCI、EI收录论文40多篇，主编教材、译著3部，参编1部，获授权国际和国家发明专利9项，受理以及公开发明专利32项，获软件著作权登记10项。