·安全技术· 文章编号：1000-3428(2018)08-0155-06 文献标志码：A 中图分类号：TP309

面向 APT 攻击的分层表示模型

樊 雷，余江明，雷英杰

（空军工程大学，西安 710051）

摘 要： 针对窃密型 APT 攻击缺乏形式化表示的问题，建立一种窃密型 APT 攻击分层表示模型 APT-HRM。参考 HARM 模型将 APT 攻击分为攻击链和攻击树上下 2 层，并对其进行形式化定义。攻击链由侦察、渗透、开采和撤出 4 个阶段组成，攻击树由攻击链各阶段所对应的攻击手段组成，APT 按照攻击链分阶段依次进行攻击。对 DUQU 2.0 APT 攻击的分析结果表明，该模型能够有效描述窃密型 APT 攻击行为。

关键词： APT 攻击；攻击链；攻击树；分层表示模型；DUQU 2.0 攻击分析

中文引用格式： 樊 雷，余江明，雷英杰. 面向 APT 攻击的分层表示模型[J]. 计算机工程，2018，44(8)：155-160.

英文引用格式： FAN Lei，YU Jiangming，LEI Yingjie. Hierarchical representation model for APT attack[J]. Computer Engineering，2018，44(8)：155-160.

Hierarchical Representation Model for APT Attack

FAN Lei，YU Jiangming，LEI Yingjie

（Air Force Engineering University，Xi'an 710051，China）

【Abstract】 In view of the lack of formal representation of the theft type APT attack，a hierarchical APT representation model is built which named APT-HRM. Referring to the HARM model，the APT attacks are divided into two layers：Attack Chain(AC) and Attack Tree(AT). The AC is composed of 4 stages：reconnaissance，infiltration，exploitation and exfiltration. The AT is composed of attack means in each stage of the AC，and the APT attacks are carried out in stages according to the AC. Analysis results of DUQU 2.0 APT attack show that，the model can effectively describe the APT attack behavior.

【Key words】 APT attack；Attack Chain(AC)；Attack Tree(AT)；hierarchical representation model；DUQU 2.0 attack analysis

DOI： 10.19678/j.issn.1000-3428.0047775

0 概述

目前，高级可持续性威胁(Advanced Persistent Threat，APT)[1]是网络空间安全面临的重大问题之一。APT 攻击由计算机和社会工程学专家共同完成，攻击者一般具有国家背景[2]。APT 具有攻击周期较长、使用一个或多个 0day 漏洞、攻击程序功能强大复杂、攻击路径多样的特点。

APT 攻击主要分为破坏型和窃密型 2 种[3]。2010 年 1 月，疑似美国和以色列的黑客组织利用 CVE-2010-2568 等多个 0day 漏洞[4]编写了著名的 Stuxnet 病毒，用其对伊朗的核设施进行破坏。2011 年10 月，黑客组织利用 CVE-2011-3402 漏洞编写 DUQU 病毒感染伊朗和苏丹的计算机并进行窃密行动。在如今的和平时期，为窃取目标的敏感信息，APT 被很多攻击者所使用[5]。

为防范窃密型 APT 的攻击，需要对其行为进行建模。本文通过对窃密型 APT 攻击进行详细分析，总结 APT 攻击各阶段的攻击手段及特点，在此基础上，建立一种 APT 攻击分层表示模型 APT-HRM(APT Hierarchical Representation Model)。在形式化定义窃密型 APT 攻击后，利用该模型对 DUQU 2.0 APT 攻击进行分析，并检验模型的性能。

1 相关工作

目前，国内外学者对 APT 建模问题的研究已经取得较多成果。文献[6]研究窃密型 APT 攻击的表示及预测方法，针对现有 APT 攻击检测和防御较困难的问题，提出一种树形结构的窃密型 APT 攻击表示方法和预测方法。文献[7]针对在移动目标防御中没有合适攻击表示方法的问题，提出一种结合攻击图和攻击树的层次攻击表示模型 HARM。文

基金项目： 国家自然科学基金(61272011，61309022)；陕西省自然科学青年基金(2013JQ8031)。

作者简介： 樊 雷(1981—)，男，讲师、博士研究生，主研方向为智能信息处理、信息融合；余江明，副教授；雷英杰，教授、博士生导师。

收稿日期： 2017-06-30 **修回日期：** 2017-08-31 **E-mail：** fanlei1771@163.com

献[8]通过对 APT 攻击手段进行分析,提出 APT 的 5 个攻击阶段。文献[9]研究 APT 的攻击特点,通过对大量 APT 攻击实例的分析,总结归纳 APT 的 4 个攻击阶段。文献[10]通过对 APT 各阶段行为的分析,总结归纳 APT 各阶段的行为特点。文献[11]针对 APT 攻击检测中缺乏推理规则的问题,通过对 APT 本体攻击行为的分析,建立 APT 攻击行为本体模型。文献[12]研究窃密型 APT 的攻击特点,针对 APT 攻击预测困难的问题,通过 Markov 链对 APT 攻击链进行建模,建立能够预测 APT 攻击的 MM-TBM 模型。

但是,上述方法在对窃密型 APT 攻击建模时,只对各攻击阶段的攻击方案进行文字描述,而没有实现形式化定义且没有对攻击方式作有效归类。为此,本文在 APT 攻击条件下对 HARM 模型进行改进,研究并建立一种窃密型 APT 攻击分层表示模型 APT-HRM。文中给出该型 APT 攻击的形式化定义,并结合一次真实的 APT 攻击事件对模型进行有效性分析。

2 APT 攻击表示模型

2.1 相关定义

将 APT 攻击分为上下 2 层,上层为攻击链(Attack Chain,AC),下层为攻击树(Attack Tree,AT)。

定义 1 APT-HRM 模型由三元组 Z 表示,$Z=(AC,AT,f)$。其中,AC 表示模型上层的 APT 攻击链,AT 表示模型下层的 APT 各阶段攻击树,$f=AC\rightarrow AT$ 表示攻击链中某阶段到对应攻击树的一一映射关系。

定义 2 攻击链 AC 位于 APT-HRM 的上层,用有向图 $B=(N,E)$ 表示。其中,N 是攻击链中各攻击阶段的有限集,$E\subseteq N\times N$ 是攻击链中连接各攻击阶段的边集,其表示 2 个攻击阶段 $n_i\in N$ 和 $n_j\in N$ 之间的迁移,即已完成 n_i 攻击阶段,将要进行 n_j 攻击阶段。

定义 3 攻击树 AT 位于 APT-HRM 的下层,用三元组 $T=(S,W,G)$ 表示。其中,S 是一组攻击方案或攻击子树的有限集,W 是一组攻击事件的有限集,其遵循树的排布规则,以($child$,$gate$,$parent$)的形式表示,$gate\in\{$AND-$gate$,OR-$gate\}$,AND-$gate$ 为逻辑“与”门,OR-$gate$ 为逻辑“或”门,G 是要达成的攻击目的,其可以是某一种攻击行为的目的,如完成主动信息侦察,也可以是阶段性攻击目的,如完成侦察阶段。

本文定义一个 2 层的 APT-HRM 模型,上层攻击链 AC 表示 APT 攻击中的各阶段,下层攻击树 AT 表示发动 APT 攻击所使用的攻击方案。APT-HRM 表示模型如图 1 所示。

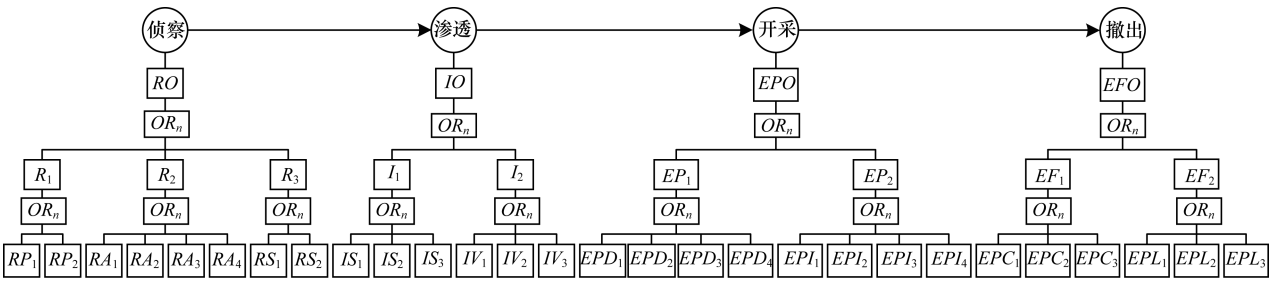

图 1 APT-HRM 模型示意图

2.2 攻击链 AC

本文建立以侦察、渗透、开采和撤出为 4 个攻击阶段的模型 RIEE。这 4 个攻击阶段构成了一个完整的攻击链,如图 2 所示。

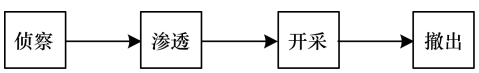

图 2 APT 攻击链

侦察阶段主要完成对攻击目标的信息搜集工作。手段主要包括被动信息侦察、主动信息侦察和半被动信息侦察,目标主要包括开放的网络端口、漏洞信息、网络拓扑结构、操作系统类型、DNS 信息、内网登陆地址、社会工程学信息、目标主要防御手段等。

渗透阶段主要利用侦察阶段获取的信息对目标进行渗透。手段主要包括社会工程学攻击和漏洞攻击,此处的漏洞一般为 0day 或 1day 漏洞,很难对其进行防范。目标主要为获得攻击目标单节点主机或某一应用系统的控制权。在该阶段,攻击者还会建立远程指挥控制中心(Command&Control,C&C),以对下一攻击阶段的行为进行远程控制。

开采阶段主要根据 C&C 指令利用单点主机或应用系统的控制权限获取敏感信息,或通过已渗透的系统对目标内部网络进行进一步渗透。手段主要有深入渗透和信息搜集。目标主要是在对象没有察觉的情况下获取其内部网络的详细信息,并进行进一步渗透和获取感兴趣的相关资料,如知识产权信息。

撤出阶段主要是将开采阶段获取的信息通过加密网络从目标网络传回攻击者手中并销毁一切攻击痕迹。手段主要包括隐秘信息回传、日志数据销毁等。目标主要是获取对象敏感信息、消除攻击痕迹。

2.3 攻击树 AT

在 APT-HRM 中,AC 中的各攻击阶段 n_i 都有与之对应的攻击树 AT_i。对于某一攻击树 AT_i,可能存在不同的子树。只有完成了 AT 中各阶段对应的攻击目标,才能转入下一个阶段。

2.3.1　侦察阶段

本节列举侦察阶段的主要攻击方案,将被动侦察方案标记为 RP,被动侦察完成记为 R_1;将主动侦察方案标记为 RA,主动侦察完成记为 R_2;将半被动侦察方案标记为 RS,半被动侦察完成记为 R_3。表 1 所示为侦察阶段 AT 的 W 三元组信息。

表 1　侦察阶段 AT 的三元组信息

编号	描述	W 三元组
RO	达成侦察目标	N/A
R_1	被动信息侦察	(R_1, OR_n^{RO}, RO)
R_2	主动信息侦察	(R_2, OR_n^{RO}, RO)
R_3	半被动信息侦察	(R_3, OR_n^{RO}, RO)
RP_1	WhoIs 查询	(RP_1, OR_n^{R1}, R_1)
RP_2	搜索引擎	(RP_2, OR_n^{R1}, R_1)
RA_1	端口扫描	(RA_1, OR_n^{R2}, R_2)
RA_2	操作系统扫描	(RA_2, OR_n^{R2}, R_2)
RA_3	网络拓扑探查	(RA_3, OR_n^{R2}, R_2)
RA_4	漏洞扫描	(RA_4, OR_n^{R2}, R_2)
RS_1	网络爬虫	(RS_1, OR_n^{R3}, R_3)
RS_2	社会工程学	(RS_2, OR_n^{R3}, R_3)

在多数已知的 APT 攻击中,R_1 和 R_3 使用较多,尤其是 RP_2 型和 RS_2 型侦察手段,在目标系统防护措施较为严密的情况下仍能够获取相关的必要信息。图 3 所示为侦察阶段的 AT 示意图。

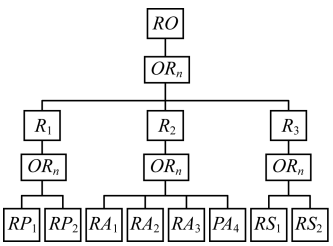

图 3　侦察阶段攻击树示意图

2.3.2　渗透阶段

本节列举渗透阶段主要的攻击方案,将社会工程学渗透方案标记为 IS,社会工程学渗透完成记为 I_1;将漏洞攻击渗透方案标记为 IV,漏洞攻击渗透完成记为 I_2。表 2 所示为渗透阶段 AT 的 W 三元组信息。

表 2　渗透阶段 AT 的三元组信息

编号	描述	W 三元组
IO	达成渗透目标	N/A
I_1	社会工程学渗透	(I_1, OR_n^{IO}, IO)
I_2	漏洞攻击渗透	(I_2, OR_n^{IO}, IO)
IS_1	网页钓鱼攻击	(IS_1, OR_n^{I1}, I_1)
IS_2	邮件钓鱼攻击	(IS_2, OR_n^{I1}, I_1)
IS_3	社会工程学字典攻击	(IS_3, OR_n^{I1}, I_1)
IV_1	硬件漏洞攻击	(IV_1, OR_n^{I2}, I_2)
IV_2	操作系统漏洞攻击	(IV_2, OR_n^{I2}, I_2)
IV_3	应用系统漏洞攻击	(IV_3, OR_n^{I2}, I_2)

此处需要注意的是目前比较流行的“水坑”攻击和“鱼叉”攻击。“水坑”攻击主要针对目标用户经常访问的应用系统(主要是网页)进行攻击,获取其管理权限并投放攻击代码。当目标用户访问该应用系统时就会触发预设的攻击代码,进而被渗透。因此,该攻击属于应用系统漏洞攻击范畴,此处的攻击一般基于 0day 漏洞,对其较难防范。“鱼叉”攻击是钓鱼攻击的一种新形式,攻击者在充分了解目标信息(包括社会关系、工作方式等)后,利用虚假信息诱骗目标运行恶意程序(通常是邮件附件)以达到渗透的目的。由于收集了目标信息,因此“鱼叉”攻击诱骗成功率比普通的钓鱼攻击高,但其仍然属于 IS_1 和 IS_2 的范畴。此外,攻击者可能伪造或窃取合法的数字证书来为恶意代码进行签名,此种情况下用户难以察觉目标在运行恶意代码。图 4 所示为渗透阶段的 AT 示意图。

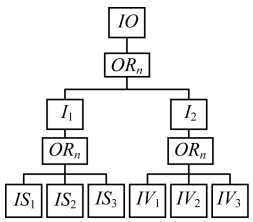

图 4　渗透阶段攻击树示意图

2.3.3　开采阶段

本节列举开采阶段主要的攻击方案,将深入渗透开采方案标记为 EPD,深入渗透开采完成记为 EP_1;将信息搜集开采方案标记为 EPI,信息搜集开采完成记为 EP_2。表 3 所示为开采阶段 AT 的 W 三元组信息。

表 3　开采阶段 AT 的三元组信息

编号	描述	W 三元组
EPO	达成开采目标	N/A
EP_1	深入渗透	(EP_1, OR_n^{EPO}, EPO)
EP_2	信息搜集	(EP_2, OR_n^{EPO}, EPO)
EPD_1	提升权限	$(EPD_1, OR_n^{EP1}, EP_1)$
EPD_2	跳板攻击	$(EPD_2, OR_n^{EP1}, EP_1)$
EPD_3	远程控制	$(EPD_3, OR_n^{EP1}, EP_1)$
EPD_4	代码驻留	$(EPD_4, OR_n^{EP1}, EP_1)$
EPI_1	硬件信息搜集	$(EPI_1, OR_n^{EP2}, EP_2)$
EPI_2	操作系统信息搜集	$(EPI_2, OR_n^{EP2}, EP_2)$
EPI_3	应用系统信息搜集	$(EPI_3, OR_n^{EP2}, EP_2)$
EPI_4	用户信息搜集	$(EPI_4, OR_n^{EP2}, EP_2)$

开采阶段是 APT 攻击的核心阶段,在渗透进入目标系统后,可以以当前节点或应用系统为基础进行深入渗透或直接进行信息搜集。在实际的 APT 攻击中,两者往往同时进行。EPI_1 一般包括网络节点 MAC 地址、处理器架构、网络拓扑结构等;EPI_2

一般包括操作系统类型、版本、漏洞信息、IP 地址等；EPI_3 一般包括应用系统口令、版本、配置情况等；EPI_4 一般包括知识产权信息、军事战略信息等。图 5所示为开采阶段的 AT 示意图。

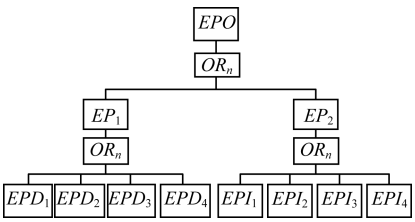

图 5 开采阶段攻击树示意图

2.3.4 撤出阶段

本节列举撤出阶段主要的攻击方案，将隐秘信息回传标记为 EFC，回传完成记为 EF_1；将日志数据销毁标记为 EFL，销毁完成记为 EF_2。表 4 所示为撤出阶段 AT 的 W 三元组信息。

表 4 撤出阶段 AT 的三元组信息

编号	描述	W 三元组
EFO	达成撤出目标	N/A
EF_1	隐秘信息回传	(EF_1, OR_n^{EFO}, EFO)
EF_2	日志数据销毁	(EF_2, OR_n^{EFO}, EFO)
EFC_1	加密通信	$(EFC_1, OR_n^{EF_1}, EF_1)$
EFC_2	匿名通信	$(EFC_2, OR_n^{EF_1}, EF_1)$
EFC_3	混淆通信	$(EFC_3, OR_n^{EF_1}, EF_1)$
EFL_1	硬件日志销毁	$(EFL_1, OR_n^{EF_2}, EF_2)$
EFL_2	操作系统日志销毁	$(EFL_2, OR_n^{EF_2}, EF_2)$
EFL_3	应用系统日志销毁	$(EFL_3, OR_n^{EF_2}, EF_2)$

EFC_1 主要通过 SSL/TLS 的加密通信、私有协议的加密通信或数据隐写技术进行通信；EFC_2 主要支持洋葱路由(TOR)[13-14]的匿名通信，也支持其他基于多跳的加密通信[15]；EFC_3 主要通过将回传通信流量混淆在正常的通信流量中，使得 IDS 等防护设备难以寻找到异常流量。由于 APT 攻击持续时间可能较长，因此攻击者可以将所需数据以十分微小的流量形式进行传输。EFL_1 主要针对硬件防护设备的日志记录进行销毁，如硬件防火墙、IPS 等；EFL_2 主要针对操作系统登录日志、操作日志等进行销毁；EFL_3 主要针对目标应用系统的操作日志进行销毁。值得注意的是，销毁只包含攻击者的日志记录时往往较困难，因此，APT 攻击者往往直接销毁目标系统的所有日志信息。图 6 所示为撤出阶段的 AT 示意图。

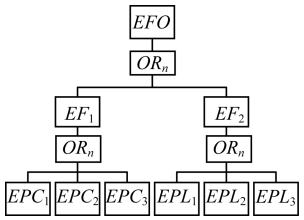

图 6 撤出阶段攻击树示意图

2.4 相关形式化示例

示例 1 对于某一 APT 攻击 A，使用 APT-HRM 模型表示为 $Z_A = (AC_A, AT_A^{N_A}, f_A)$。其中，$AC_A$ 表示攻击 A 中的攻击链，$AT_A^{N_A}$ 表示攻击 A 中攻击阶段 N_A 对应的攻击树，f_A 表示攻击 A 中上层 AC_A 中的攻击阶段 N_A 到下层 $AT_A^{N_A}$ 的一一映射关系，即 $f_A = N_A \rightarrow AT_A^{N_A}, N_A \in N$。

示例 2 在 APT-HRM 中，攻击链 AC 的有向图表示为 $C = (\{n_R, n_I, n_{EP}, n_{EF}\}, \{(n_R, n_I), (n_I, n_{EP}), (n_{EP}, n_{EF})\})$。其中，$n_R$ 是侦察阶段，n_I 是渗透阶段，n_{EP} 是开采阶段，n_{EF} 是撤出阶段，(n_i, n_j) 表示从 n_i 阶段转移到 n_j 阶段。

示例 3 在侦察阶段的攻击树中，要完成 RO，则 $T_R = (\{T_{R_1}, T_{R_2}, T_{R_3}\}, \{(T_{R_1}, OR_n^{RO}, OR), (T_{R_2}, OR_n^{RO}, OR), (T_{R_3}, OR_n^{RO}, OR)\}, RO)$；要完成 R_1，则 $T_{R_1} = (\{RP_1, RP_2\}, \{(RP_1, OR_n^{R_1}, R_1), (RP_2, OR_n^{R_1}, R_1)\}, R_1)$；要完成 R_2，则 $T_{R_2} = (\{RA_1, RA_2, RA_3, RA_4\}, \{(RA_1, OR_n^{R_2}, R_2), (RA_2, OR_n^{R_2}, R_2), (RA_3, OR_n^{R_2}, R_2), (RA_4, OR_n^{R_2}, R_2)\}, R_2)$；要完成 R_3，则 $T_{R_3} = (\{RS_1, RS_2\}, \{(RS_1, OR_n^{R_3}, R_3), (RS_2, OR_n^{R_3}, R_3)\}, R_3)$。

3 DUQU 2.0 APT 攻击的 APT-HRM 表示

著名网络安全厂商卡巴斯基实验室于 2015 年宣布自身遭受了代号为 DUQU 2.0 的 APT 攻击，导致其部分知识产权信息被窃取。其自身经过详细地分析，于 2015 年 6 月公布了攻击的技术细节报告[16]。本文利用 APT-HRM 对此次攻击进行建模与分析，以检验 APT-HRM 模型的性能。

3.1 攻击链

DUQU 2.0 攻击链包含 RIEE 的全部 4 个阶段。在侦察阶段，攻击者利用各种方法获取了卡巴斯基实验室亚太区某员工的详细信息(至少包括上下级关系、邮箱地址、内部应用系统信息等)；在渗透阶段，攻击者运用社工方法诱骗实验室工作人员打开带有恶意附件的邮件，并利用 3 个 0day 漏洞获取了

系统的控制权;在开采阶段,攻击者利用 0day 漏洞将自身权限提高到管理员级别,并利用被感染的计算机作为跳板感染网络内其他计算机,然后建立 C&C 对开采行动进行远程控制,同时对网络拓扑结构、操作系统信息、内网应用系统信息和知识产权信息进行搜集;在撤出阶段,攻击者利用图片数据隐写技术和流量混淆技术与 C&C 建立隐蔽通信,以此回传相关信息,同时对入侵记录进行销毁。

3.2　攻击树

3.2.1　侦察阶段

文献[16]没有分析出攻击者在侦察阶段所完成的工作,但是怀疑此次攻击是基于电子邮件的“鱼叉”式攻击。由此可知,在侦察阶段攻击者至少知道了目标(卡巴斯基实验室员工)的社会关系、邮件地址、计算机操作系统(攻击使用的 0day 漏洞)、初步的网络拓扑结构(对核心内网进行渗透)。因此,攻击者至少使用了主动信息侦察和半被动信息侦察,攻击树可表示为 $T_R=(\{T_{R_2},T_{R_3}\},\{(T_{R_2},OR_n^{RO},OR),(T_{R_3},OR_n^{RO},OR)\},RO)$。主动信息侦察攻击树可表示为 $T_{R_2}=(\{RA_2,RA_3,RA_4\},\{(RA_2,OR_n^{R_2},R_2),(RA_3,OR_n^{R_2},R_2),(RA_4,OR_n^{R_2},R_2)\},R_2)$;半被动信息侦察攻击树可表示为 $T_{R_3}=(RS_2,(RS_2,OR_n^{R_3},R_3),R_3)$。

3.2.2　渗透阶段

在渗透阶段,攻击者采用“鱼叉”式钓鱼攻击方法,利用钓鱼邮件将带有攻击载荷的 Word 文档发送给目标并诱骗目标打开该文档,然后利用 CVE-2014-4148 漏洞获取系统控制权。因此,此过程中攻击者至少使用了网页钓鱼攻击、邮件钓鱼攻击、操作系统漏洞攻击和应用系统漏洞攻击,攻击树可表示为 $T_I=(\{T_{I_1},T_{I_2}\},\{(T_{I_1},OR_n^{IO},IO),(T_{I_2},OR_n^{IO},IO)\},IO)$。社会工程学渗透攻击树可表示为 $T_{I_1}=(IS_1,IS_2,\{(IS_1,OR_n^{I_1},I_1),(IS_2,OR_n^{I_1},I_1)\},I_1)$;漏洞攻击渗透攻击树可表示为 $T_{I_2}=(\{IV_2,IV_3\},\{(IV_2,OR_n^{I_2},I_2),(IV_3,OR_n^{I_2},I_2)\},I_2)$。

3.2.3　开采阶段

在开采阶段,攻击者进行深入渗透和信息搜集。攻击者首先利用 CVE-2014-6324 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 C&C 控制的远程后门程序。DUQU 2.0 使用的代码驻留方式十分特别,几乎没有存储于磁盘的文件,绝大部分代码运行在内存中,因此,目标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操作的后门程序,一旦发生载荷丢失现象,可以立即对其进行重新安装。

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,主要包括深入渗透和信息搜集 2 类。其中,信息搜集的对象主要包括 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,运行进程列表、活跃终端会话、所有网络共享和安装的程序、域管理员 SID 及密码 HASH 等操作系统信息,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,开采阶段的攻击树可表示为 $T_{EP}=(\{T_{EP_1},T_{EP_2}\},\{(T_{EP_1},OR_n^{EPO},EPO),(T_{EP_2},OR_n^{EPO},EPO)\},EPO)$。深入渗透攻击树可表示为 $T_{EP_1}=(\{EPD_1,EPD_2,EPD_3,EPD_4\},\{(EPD_1,OR_n^{EP_1},EP_1),(EPD_2,OR_n^{EP_1},EP_1),(EPD_3,OR_n^{EP_1},EP_1),(EPD_4,OR_n^{EP_1},EP_1)\},EP_1)$;信息搜集攻击树可表示为 $T_{EP_2}=(\{EPI_1,EPI_2,EPI_3,EPI_4\},\{(EPI_1,OR_n^{EP_2},EP_2),(EPI_2,OR_n^{EP_2},EP_2),(EPI_3,OR_n^{EP_2},EP_2),(EPI_4,OR_n^{EP_2},EP_2)\},EP_2)$。

3.2.4　撤出阶段

在撤出阶段,攻击者进行隐秘信息回传和日志数据销毁。在隐秘信息回传中,攻击者使用 Windows 管道和邮槽并通过私有协议进行加密通信,还通过隐写技术将信息封装在正常的图片中进行传输以达到流量混淆;在日志数据销毁中,攻击者对操作系统的日志信息进行清除,同时对被攻击节点上的用户邮箱和浏览器记录进行清除。因此,撤出阶段的攻击树可表示为 $T_{EF}=\{T_{EF_1},T_{EF_2}\},\{(EF_1,OR_n^{EFO},EFO),(EF_2,OR_n^{EFO},EFO)\},EFO)$。隐秘信息回传攻击树可表示为 $T_{EF_1}=(\{EFC_1,EFC_3\},\{(EFC_1,OR_n^{EF_1},EF_1),(EFC_3,OR_n^{EF_1},EF_1)\},EF_1)$;日志数据销毁攻击树可表示为 $T_{EF_2}=(\{EFL_2,EFL_3\},\{(EFL_2,OR_n^{EF_2},EF_2),(EFL_3,OR_n^{EF_2},EF_2)\},EF_2)$。

3.3　APT-HRM 表示

DUQU 2.0 APT 攻击 $Z_A=(AC_A,AT_A^{N_A},f_A)$。其中,$A$ 表示 DUQU 2.0 APT 攻击。AC_A 中 $C=(N_A,E_A)$,

$N_A=\{n_R,n_I,n_{EP},n_{EF}\}$, $E_A=\{(n_R,n_I),(n_I,n_{EP}),(n_{EP},n_{EF})\}$。$AT_A^{N_A}=\{T_R,T_I,T_{EP},T_{EF}\}$。$f_A=\{n_R\rightarrow T_R,n_I\rightarrow T_I,n_{EP}\rightarrow T_{EP},n_{EF}\rightarrow T_{EF}\}$。因此,APT-HRM 模型完全能够表示 DUQU 2.0 APT 攻击。

4 结束语

本文建立一种窃密型 APT 攻击分层表示模型 APT-HRM。APT-HRM 对 APT 攻击进行了形式化定义,将 APT 攻击分为攻击链和攻击树 2 层。攻击链各阶段有其对应的由不同攻击策略和方法组成的攻击树,只有完成当前阶段攻击树中的攻击目标才能转入下一个攻击阶段。因此,可以针对各阶段的攻击手段进行防范,以切断 APT 攻击链并最终阻止 APT 攻击。对 DUQU 2.0 APT 攻击的建模分析结果表明,该模型能够有效描述窃密型 APT 攻击行为,可为 APT 攻击的预测和防御提供参考。

参考文献

[1] ROSS R. Managing information security risk:organization, mission and information system view[EB/OL]. [2017-06-30]. https://ws680. nist. gov/publication/get _ pdf. cfm?pub_id = 908030.

[2] AUTY M. Anatomy of an advanced persistent threat[J]. Network Security,2015(4):13-16.

[3] 胡 彬,王春东,胡思琦,等. 基于机器学习的移动终端高级持续性威胁检测技术研究[J]. 计算机工程,2017,43(1):241-246.

[4] KAUR R,SINGH M. A survey on zero-day polymorphic worm detection techniques[J]. IEEE Communications Surveys and Tutorials,2014,16(3):1520-1549.

[5] 潘道欣,王轶骏,薛 质. 基于网络协议逆向分析的远程控制木马漏洞挖掘[J]. 计算机工程,2016,42(2):146-150.

[6] 张小松,牛伟纳,杨国武,等. 基于树型结构的 APT 攻击预测方法[J]. 电子科技大学学报,2016,45(4):582-588.

[7] 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.

[8] DOHERTY S, BANERJEE D. Orchestrating software defined networks (SDN) to disrupt the APT kill chain[EB/OL]. [2017-06-30]. https://www. rsaconference. com/events/us15/agenda/sessions/1555/orchestrating-software-defined-networks-sdn-to.

[9] LI M,HUANG W,WANG Y,et al. The study of APT attack stage model[C]//Proceedings of 2016 IEEE/ACIS International Conference on Computer and Information Science. Washington D. C. ,USA:IEEE Press,2016:1-5.

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

[11] CHOI J,CHOI C,LYNN H M,et al. Ontology based APT attack behavior analysis in cloud computing[C]//Proceedings of the 10th International Conference on Broadband and Wireless Computing,Communication and Applications. Washington D. C., USA: IEEE Press, 2015:375-379.

[12] IOANNOU G,LOUVIERIS P,CLEWLEY N,et al. A Markov multi-phase transferable belief model: an application for predicting data exfiltration APTs[C]//Proceedings of International Conference on Information Fusion. Washington D. C., USA: IEEE Press, 2013: 842-849.

[13] KOCH R, GOLLING M, RODOSEK G D. How anonymous is the tor network? a long-term black-box investigation[J]. Computer,2016,49(3):42-49.

[14] GEHL R W. Power/freedom on the dark Web:a digital ethnography of the dark Web social network[J]. New Media and Society,2016,18(7):1219-1235.

[15] 胡 飞,范建华,魏祥麟,等. 基于节点状态跳转统计分析的干扰攻击检测算法[J]. 计算机工程,2017,43(7):156-162.

[16] GReAT. The DUQU 2.0 Technical Details[R]. Moscow, Russia:Kaspersky Lab,2015.

编辑 吴云芳

(上接第 154 页)

[18] 张玉磊,张灵刚,张永洁,等. 匿名 CLPKC-TPKI 异构签密方案[J]. 电子学报,2016,44(10):2432-2439.

[19] 刘景伟,张俐欢,孙 蓉. 异构系统下的双向签密方案[J]. 电子与信息学报,2016,38(11):2948-2953.

[20] 金春花. 新的基于身份的混合签密[D]. 西安:西安电子科技大学,2011.

[21] 俞惠芳,杨 波. 可证安全的无证书混合签密[J]. 计算机学报,2015,38(4):804-813.

[22] 苏万力,张跃宇,张晓红,等. 无证书盲签名方案[J]. 电子科技大学学报,2009,38(4):533-536.

[23] 龙士工,伍 岳,王利军. 基于门限的无可信中心的盲签名方案[J]. 计算机应用研究,2010,27(7):2657-2660.

[24] 秦晓君. 盲签名设计及其在电子商务中的应用[D]. 西安:长安大学,2011.

[25] 俞惠芳,王彩芬,王之仓. 基于 DLP 的自认证盲签密方案[J]. 计算机工程与应用,2010,46(23):119-121.

[26] 俞惠芳,王彩芬,杨 林,等. 基于无证书的盲签密方案[J]. 计算机应用与软件,2010,27(7):71-73.

[27] 宋明明,张 彰,谢文坚. 没有对运算的无证书盲签密方案[J]. 广西民族大学学报(自然科学版),2011,17(1):64-67.

编辑 顾逸斐