定向网络攻击追踪溯源层次化模型研究

刘潮歌[1,2], 方滨兴[3,4], 刘宝旭[1,2*], 崔 翔[4], 刘奇旭[1,2]

[1]中国科学院信息工程研究所, 北京 中国 100093
[2]中国科学院大学网络空间安全学院, 北京 中国 100049
[3]电子科技大学广东电子信息工程研究院, 广东东莞 中国 523808
[4]广州大学网络空间先进技术研究院, 广州 中国 510006

摘要 定向网络攻击对网络空间安全构成了极大的威胁, 甚至已经成为国家间网络对抗的一种主要形式。本文认为定向网络攻击难以避免, 传统的以识别并阻断攻击为核心的防御体系不能很好地应对复杂先进的定向网络攻击, 遂提出将追踪溯源作为威慑性防御手段。本文给出了定向网络攻击追踪溯源的形式化定义和分类; 充分借鉴了网络欺骗等领域的研究成果, 提出通过构建虚实结合的网络和系统环境, 采用主被动相结合的方式, 追踪溯源定向网络攻击; 构建了包括网络服务、主机终端、文件数据、控制信道、行为特征和挖掘分析六个层次的定向网络攻击追踪溯源模型, 并系统阐述了模型各层次的内涵及主要技术手段; 以此模型为基础, 建立了以“欺骗环境构建”、“多源线索提取”、“线索分析挖掘”为主线的追踪溯源纵深体系, 多维度追踪溯源定向网络攻击; 结合现有攻击模型、追踪溯源理论和典型溯源案例, 论证了所建立的模型的有效性。

关键词 定向网络攻击; 追踪溯源; 网络欺骗; APT
中图法分类号 TP393.0 DOI 号 10.19363/J.cnki.cn10-1380/tn.2019.07.01

A Hierarchical Model of Targeted Cyber Attacks Attribution

LIU Chaoge[1, 2], FANG Binxing[3, 4], LIU Baoxu[1, 2*], CUI Xiang[4], LIU Qixu[1, 2]

[1]Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2]School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
[3]Institute of Electronic and Information Engineering of University of Electronic Science and Technology of China in Guangdong, Dongguan Guangdong 523808, China
[4]Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou 510006, China

Abstract In recent years, the evolving targeted cyber attacks have posed a great threat to cyber security, and even become a major form of cyberwar among many countries. However, current defense methodologies, which generally focus on discovering and then blocking the known attacks, cannot deal with these advanced targeted cyber attacks effectively. To solve the problems to some degree, in this paper, we introduce an attribution method as an alternative methodology. Firstly, we give a formal definition and classification of *Targeted Cyber Attacks Attribution,* and then we introduce some research works on related fields (such as cyber deception) to attribution. We further deploy a well-designed Virtual-Actual attribution environment and attribute targeted attacks with both active and passive methods. To achieve this goal, we establish a new attribution model as well as build an attribution-in-depth system. The proposed model includes six levels including network services, hosts and terminals, files and data, command and control channels, behavioral characteristics as well as mining and analyzing. We describe the theoretical and technical details of each level. With the main thread of deception environment construction, multi-source clue extraction and data mining and analyzing, the attribution-in-depth system is designed to attribute targeted attacks from multiple dimensions. At last, we evaluate the proposed model from multiple perspectives including existing attack model, attribution theory and some typical attribution cases, and conclude that the proposed model can offer an effective way for targeted cyber attacks attribution.

Key words targeted cyber attack; attribution; cyber deception; APT

通讯作者: 刘宝旭, 博士, 研究员, Email:liubaoxu@iie.ac.cn。

本课题得到中国科学院网络测评技术重点实验室和网络安全防护技术北京市重点实验室资助; 得到国家重点研发计划(No.2016QY08D1602), 中国科学院青年创新促进会, 中国科学院战略先导 C 类(No.XDC02040100, No.XDC02030200, No.XDC02020200)课题资助。
收稿日期: 2018-02-03; 修改日期: 2018-06-21; 定稿日期: 2019-06-06

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

1 引言

定向网络攻击是指针对特定目标(用户、公司或组织等)发起的网络攻击, 直接目的是隐蔽窃密或破坏关键设施。定向网络攻击对网络空间安全构成了极大的威胁, 近年来备受关注的 APT(Advanced Persistent Threat, 高级持续性威胁)就是定向网络攻击的一种高级表现形式, 可以看作是定向网络攻击的一个真子集[1]。网络攻击追踪溯源, 美国军方的说法是“ Attribution ”, 中文直译为“ 归因 ”, 一般指追踪网络攻击源头、溯源攻击者的过程。也有文献将“ Traceback ”和“ Source Tracking ”视为“ Attribution ”之意。

以 APT 为代表的定向网络攻击, 其典型目的是获取高额的政治、经济回报, 被认为是国家间或组织间网络对抗的表现形式: 2010 年, 震网攻击了伊朗的核工业基础设施, 造成约 1000 台铀浓缩离心机故障[2-3], 迟滞了伊朗核计划, 这是第一起引起广泛关注的定向网络攻击事件。2015 年初起, 孟加拉等多国的 SWIFT 银行转账系统先后遭到攻击, 累计造成了近 1 亿美元的经济损失[4]。2015 年, 乌克兰一家电力公司的 SCADA 系统遭到入侵, 造成 22.5 万用户长达数小时的电力中断[5], 给民众生活和国家安全造成了严重危害。2016 年美国大选期间, “ 邮件门 ”丑闻引起美国政坛的巨大震动, 影响了美国大选走向[4]。还有报告显示 2017 年法国大选、2016 年台湾民选、2014 年乌克兰大选, 也不同程度地受到了 APT 的干扰[6-8]。

定向网络攻击的危害毋庸赘言, 如何有效应对定向网络攻击已成为学术界和工业界共同关注的焦点问题。现有的网络安全防御以识别并阻断网络攻击为核心, 力求拒威胁于内网之外。但是随着定向网络攻击的出现与发展, 防御者逐渐认识到“ 定向网络攻击难以避免 ”:

第一, 从网络系统本身看, 其具有确定性、静态性和同构性[9-10], 攻击者既可以建立模拟环境(包括目标系统和安全设备)分析测试目标系统的脆弱性, 也可以直接地反复尝试渗透目标系统。每一次攻击失败都为攻击者提供了改进经验, 却不能帮助防御者加固系统防护。

第二, 从攻防不对称性看, 网络防御符合“ 木桶原理 ”, 安全防御需要面面俱到, 而攻击者只需要找到并成功利用目标系统的若干个脆弱点。

第三, 从纯技术角度看, 检测未知攻击手段(如 0day)是现有安全防护手段普遍面临的难题, 即攻击者有机会凭借绝对技术优势绕过现有防御体系。此外, 安全防护系统和设备本身也可能存在漏洞。

第四, 从战术技巧角度看, “ 人 ”已经成为网络安全防护中最薄弱的环节之一, 运用社会工程学手段攻陷目标网络, 在定向网络攻击中屡见不鲜。

第五, 从实际案例来看, 正如前文所述, 无论是物理隔离的核基础设施内网, 相对封闭的 SWIFT 和 SCADA 等专用系统, 还是严密保护的政要的个人资产, 都存在被入侵、被攻陷的案例。

本文对定向网络攻击追踪溯源的研究, 正是建立在“ 定向网络攻击难以避免 ”这一合理假设的基础之上。在该前提下, 定向网络攻击的防御不能单纯地依赖识别和阻断, 而是需要把追踪溯源补充为应对定向网络攻击的重要手段: 在技术层面上, 追踪溯源可以及时确定网络攻击目的和使用的技术手段, 不仅能够有效提高网络防御的有效性和针对性, 还能加深对 TTP(Tactics, Techniques, Procedures, 战术, 技术, 程序)的理解, 提高网络空间积极防御能力。在战术层面上, 追踪溯源可以为解决国家间网络空间安全争端提供取证支撑, 是捍卫国家网络空间主权[11]必要手段; 在战略层面上, 追踪溯源攻击者的真实身份和幕后组织者, 可以提升网络空间安全防御的威慑力, 达到“ 不战而屈人之兵 ”的防御效果。此外, 本文提出构建的虚实结合的追踪溯源环境还兼具发现定向网络攻击、消耗攻击者资源的能力, 从而在一定程度上避免真实信息系统遭到攻击。

然而, 定向网络攻击追踪溯源的现状不容乐观。表 1 总结了近年来一些影响广泛的 APT 事件, 虽然出现了若干影响较广泛的追踪溯源案例[12-15], 但是总体上看, 安全界并没有很好地解决定向网络攻击追踪溯源问题。针对定向网络攻击的追踪溯源这一实际需求, 本文提出了若干新的解决思路, 并形成模型。本文主要贡献总结如下:

1. 给出了定向网络攻击追踪溯源的形式化定义, 并将追踪溯源技术做了分类;

2. 引入网络欺骗、Web 追踪等技术, 提出构建虚实结合的网络和系统环境, 采用主被动相结合的方式追踪溯源定向网络攻击;

3. 建立了定向网络攻击追踪溯源层次化模型, 分别阐述了各层次的含义, 并总结了现有技术手段和工作成果;

4. 基于定向网络攻击追踪溯源层次化模型, 提出建立追踪溯源纵深体系, 多维度追踪溯源定向网络攻击;

5. 结合现有攻击模型和追踪溯源理论, 评价了所提出的定向网络攻击追踪溯源层次化模型。

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

表 1 近年重要 APT 事件及追踪溯源结论

Table1 Influential APT events and attribution conclusions in recent years

名称	发现时间	攻击目标	主要影响	追踪溯源情况
Stuxnet[2]	2010 年	伊朗核工业基础设施	成功破坏了 1000 多台铀浓缩离心机, 迟滞了伊朗核计划	未形成明确的追踪溯源结论, 但美国官员主动承认是美国和以色列所为[16]
Duqu[17]	2011 年	工控领域元器件制造商	收集大量情报资料和资产信息	未形成明确的追踪溯源结论
Red October[18]	2012 年	多国外交使馆、政府和科研机构	包括美国、巴西、澳大利亚在内的 39 个国家受到影响	未形成明确的追踪溯源结论
APT1[12]	2013 年	全球 141 个组织, 涉及 20 个主要行业	窃取数百 TB 的信息	Mandiant 公司在其研究报告中形成了明确的追踪溯源结论[12]
SandWorm[19]	2014 年	北约、欧盟、乌克兰、波兰	信息窃取, 破坏工控系统, 与乌克兰电网事件有关	未形成明确的追踪溯源结论
APT28[13-14]	2014 年	欧美和前苏联国家, 包括政府和军事国防机构、媒体以及与俄罗斯当局不同政见者	干扰美国、乌克兰和法国大选, 攻击法国电视台, 入侵世界反兴奋剂组织数据库	FireEye 公司在其研究报告中形成了明确的追踪溯源结论[13, 14]
Turla[20]	2014 年	政府机构、大使馆、军事、教育、科研、制药公司等	以收集情报为主, 影响哈萨克斯坦、俄罗斯、法国、中国、越南、美国等 45 个国家	未形成明确的追踪溯源结论
Duqu 2.0[21]	2015 年	西欧、中东、亚洲	窃听伊核问题高层谈话, 潜入卡巴内网	未形成明确的追踪溯源结论
Equation Group[22]	2015 年	多国政府、外交机构, 电信、航空、能源、军工企业	影响全球 30 多个国家, 感染成千上万受害者	未形成明确的追踪溯源结论, 但结合斯诺登[23]和“影子经纪人”[24]的泄密, 确定该组织隶属美国国家安全局[25-27]
Naikon[15]	2015 年	东南亚多国军事、外交和经济目标, 以及东盟等国际组织	活跃的 5 年内, 大量收集了关于政治、经济的情报	ThreatConnect 和 DGI 公司在其研究报告中形成了明确的追踪溯源结论[15]
Project Sauron[28-29]	2016 年	针对中国、俄罗斯等政府机构、民生企业和个人	针对中俄发动数十起攻击, 可以从隔离内网窃取重要数据	未形成明确的追踪溯源结论

本文引用了部分已公开的定向网络攻击追踪溯源结论, 但并不等同于认定这些结论就是事实: 因涉及利益的特殊性, 既存在攻击者伪装嫁祸于无辜第三方的可能, 也存在溯源者刻意引导舆论的可能。这也恰好从侧面证明了研究准确追踪溯源技术的重要性。本文不讨论所引用的追踪溯源结论的真实性, 也不对这些结论持任何观点, 只基于公开资料研究其涉及的关键技术。

2 定向网络攻击追踪溯源的形式化定义和分类

2.1 定义

Wheeler 等曾给出了经典的网络攻击追踪溯源的一般性定义: 确定攻击者或者攻击跳板的身份及位置; 其中, 身份可以是姓名、账号、昵称, 以及任何能够和自然人相关联的信息; 位置既包括物理位置, 也包括虚拟地址, 如 IP 地址或以太网地址[30]。受时代的局限, 这个定义适用于非定向网络攻击, 而没有考虑定向网络攻击的目的性、复杂性和持续性。在此背景下, 本文给出定向网络攻击追踪溯源的一般性描述:

定义 1. 定向网络攻击追踪溯源(Targeted Cyber Attacks Attribution)。在定向网络攻击的各个阶段, 包括攻击完成之后, 通过一定的技术手段完成以下三级目标: 确定攻击的目的; 确定攻击实施过程; 确定攻击者的身份。在上述定义的基础上, 给出网络攻击追踪溯源的形式化定义 *Targeted Cyber Attacks Attribution={Stage, Attribution Method, Target, Implementation, Identity}*。

1) *Stage*。定向网络攻击具有持续性, 因此追踪溯源也应该相应地覆盖到定向网络攻击的各个阶段, 包括攻击完成之后。结合“网络入侵杀伤链”(Intrusion Kill Chain)模型[31], 有 *Stage={Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, Action on Objectives, Accomplishment}*, 分别对应于定向网络攻击的目标侦查、武器生产、载荷投递、突防利用、安装植入、命令控制、任务执行, 以攻击完成阶段。

2) *Attribution Method*。防御者追踪溯源定向网络攻击所采用的技术手段, 本文将其划分为主动追踪溯源和被动追踪溯源两大类, 即 *Attribution Me-*

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

thod={*Active Attribution, Passive Attribution*}。

3) *Target*。定向网络攻击的目标, 包括网络破坏和网络窃密, 即 *Target*={*Sabotage, Espionage*}。

4) *Implementation*。定向网络攻击的过程, 包括使用的攻击资源(Resource)和攻击路径(Path), 定向网络攻击具有复杂性, 使用的攻击资源和路径非常丰富。攻击资源指定向网络攻击中使用到的跳板、服务、工具、漏洞、账号、域名等一切资源, 有 *Resource*={*Hop, Service, Tool, Vulnerability, Account, Domain, et al.*}。攻击路径是由多条子攻击路径构成的集合, 有 *Path*={*Path1, Path2, ..., PathN*}。每条子攻击路径, 又是各个子攻击(Attack)的有序集合, 于是有<*PathN, R*>={*Attacks1, Attack2, ..., AttackN*}, *R* 表示各子攻击的先后顺序。

5) *Identity*。定向网络攻击者的身份, 包括攻击者作为自然人的物理身份信息和作为网络用户的虚拟身份信息, 也包括攻击者所属组织的物理和虚拟背景信息, 有 *Identity*={*Person, Organization*}。

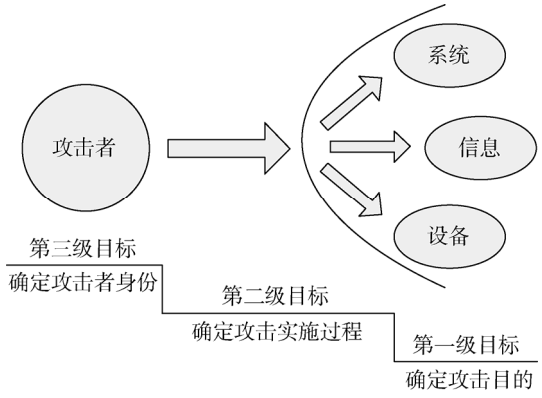


图 1 定向网络攻击追踪溯源三级目标

Figure 1 3-goals of targeted cyber attacks attribution

2.2 分类方法

本文将定向网络攻击追踪溯源分为“被动追踪溯源”和“主动追踪溯源”两类, 并作如下一般性描述:

定义 2. 被动追踪溯源(Passive Attribution)。溯源者不干扰攻击过程, 仅利用攻击者主动暴露的线索求解追踪溯源各级目标的过程。

定义 3. 主动追踪溯源(Active Attribution)。溯源者有意识地部署环溯源境或释放溯源工具, 干扰攻击者的行为, 导致其产生原定计划外的攻击动作或网络流量, 从而探测或收集额外的攻击者线索, 并利用上述信息求解追踪溯源各级目标的过程。

被动溯源通常以记录日志和流量为主要手段, 部署简单, 但缺点也显而易见: 获得的线索是“攻击者可控的”, 即便在防御者做出最大努力、记录全部日志和流量的前提下, 也有可能无法得到溯源关键线索。主动追踪溯源则是按照溯源者的意愿, 尝试获得溯源关键线索, 缺点是技术难度大。从实施时间来看, 被动追踪溯源包括攻击前部署、攻击中记录和攻击后回溯三个阶段; 而主动追踪溯源则主要包括攻击前部署和攻击中实施两个阶段。从实施空间来看, 被动追踪溯源主要发生在防御者一侧, 而主动追踪溯源既可以发生在防御者一侧(如蜜罐主机), 也可以发生在攻击者一侧(如攻击者浏览器、主机)。

3 定向网络攻击追踪溯源技术

本章首先综述现有网络攻击追踪溯源技术, 并指出其在应对定向网络攻击追踪溯源方面的不足, 进而分析威胁情报、Web 追踪和网络欺骗等技术在主动追踪溯源定向网络攻击方面的应用。

3.1 现有追踪溯源技术综述

陈周国等[32]和姜建国等[33]的工作比较具有代表性, 他们分别从各自角度综述了现有网络攻击追踪溯源技术。

Cohen D 等[34]曾将网络攻击追踪溯源划分为追踪溯源攻击主机、追踪溯源攻击控制主机、追踪溯源攻击者、追踪溯源攻击组织机构四个级别。陈周国等[32]则在此基础上, 详细阐述了各级别追踪溯源面临的具体问题, 并综述了为实现各级目标可以采取的技术手段。但是该工作没有区分攻击的指向性, 因而所综述的技术手段在应对定向网络攻击追踪溯源方面存在局限性: 首先, 在追踪溯源第一层次上使用的 Input Debugging[35]、Itrace[36]、PPM[37]、DPM[38]、SPIE[39]等方法, 是网络数据包层面的技术方法, 主要针对非定向网络攻击(如 DDoS), 而定向网络攻击频繁使用跳板主机、跳板网络和公共网络服务, 因而上述方法的追踪溯源能力有限; 其次, 第二层次上使用的内部监测、日志分析、网络流分析、事件响应分析等技术, 以被动追踪溯源手段为主, 缺少对追踪溯源关键线索的主动获取, 收集到的线索有限, 难以有效溯源复杂的定向网络攻击; 再次, 在第三层次上总结的自然语言文档分析、Email 分析、聊天记录分析、攻击代码分析、键盘信息分析等技术, 能够在一定程度上帮助追踪溯源定向网络攻击, 但这些分析技术基于对已知样本和数据的挖掘利用, 并没有提及如何高效地捕获这些样本和数据。

姜建国等[33]根据不同的攻击场景, 将网络攻击追踪溯源划分为虚假 IP 追踪、Botnet 追踪、匿名网络追踪、跳板追踪和局域网追踪 5 类问题, 并将解决

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

这五类问题的技术方法归纳为 4 种类型: 包标记、流水印、日志记录和渗透测试。从问题划分来看, 该工作没有充分考虑在定向网络攻击这一特定场景下的追踪溯源问题, 因此所归纳总结的技术方法更倾向于追踪溯源非定向网络攻击。文献综述的包标记方法主要包括 Itrace、PPM、DPM 技术, 如前文所述, 作为网络数据包层面的追踪溯源方法, 难以应对复杂的定向网络攻击。流水印技术不需要修改协议, 也适用于加密流量, 甚至可以用来追踪溯源一些以匿名网络为跳板的定向网络攻击[40]。但是流水印技术需要大量匿名网络基础设施的支持, 因而不易实施, 同时在技术上要保证水印检测的准确率也有一定难度。日志记录技术则是一种被动追踪溯源方法, 存在所记录的信息有限、可能被攻击者篡改的问题。渗透测试的方法可以为定向网络攻击的追踪溯源提供关键突破, 但是技术难度大并且存在司法可信性方面的疑问, 目前已公开的追踪溯源报告中, 很少提及此类方法。

综上所述, 现有的网络攻击追踪溯源研究成果, 在应对定向网络攻击追踪溯源问题上存在以下不足。

总体来看, 现有研究成果大多面向非定向网络攻击, 而缺少专门面向定向网络攻击追踪溯源的理论和技术的研究。定向网络攻击是应用和业务层面上而非网络层面上的攻击, 更具隐蔽性、匿名性、持久性和复杂性, 追踪溯源的难度更大。同时, 定向网络攻击使用的攻击工具和攻击方法, 也和非定向网络攻击有着显著的区别。因此, 在定向网络攻击追踪溯源理论和技术方面, 都需要相应地创新。

从技术细节来看, 现有技术手段以被动追踪溯源技术为主, 缺少主动获取追踪溯源关键信息方面的研究。网络攻击的隐蔽性和匿名性符合“木桶原理”, 因此, 追踪溯源的突破往往取决于若干少量的核心关键线索。被动追踪溯源收集到的是攻击者有意或无意泄露的信息, 线索质量难以满足溯源方的预期。主动溯源则是主动出击, 在司法允许的范围内, 结合陷阱、诱捕、欺骗和软硬件特性利用等方法, 同时在攻击目标和攻击者两端获取高质量的关键溯源线索。

从系统性来看, 各类追踪溯源技术独立使用、各自为战, 而缺少定向网络攻击追踪溯源的整体模型研究。学术界和工业界在追踪溯源方面积累了大量的研究成果和成功案例, 同时在其他领域也出现了较好的思路和技术可以借鉴。模型研究作为基础性工作, 可以有效整合现有策略、资源和技术手段, 并应用于网络和系统的各个层面上, 形成面向追踪溯源的纵深化防御体系。

3.2 威胁情报技术

为了更加准确高效地追踪溯源网络攻击, 工业界提出了威胁情报(Threat Intelligence)这一概念。Gartner 曾给出了比较通用的威胁情报定义: 威胁情报是一种基于证据的知识, 包括威胁相关的上下文信息(Context)、威胁所使用的方法机制(Mechanisms)、威胁指标(Indicators)、攻击影响(Implications)以及应对建议(Actionable advices)等。威胁情报描述了现存的或者即将出现的针对资产的威胁或危险, 并可以用于通知受害一方针对威胁或危险采取应对措施[41]。

2013 年, David J. Bianco[42]在总结威胁指标(IOC, Indicator of Compromise)类型及其攻防对抗价值的基础上, 建立了威胁情报价值金字塔模型(The Pyramid of Pain), 该模型揭示了防御者追踪溯源到不同的威胁指标时, 会导致攻击者付出的代价大小。2015 年, 杨泽明等[43]明确指出“威胁情报的共享利用将是实现攻击溯源的重要技术手段”。目前, 一些安全公司建立了各自的在线威胁情报平台(如文献[44-48]), 提供查询和分析服务, 帮助追踪溯源网络攻击。

威胁情报在定向网络攻击追踪溯源方面的优势在于其海量多来源知识库以及情报的共享机制。这些情报可以为追踪溯源工作提供有力支撑: 防御者将已掌握的溯源线索作为输入传递给威胁情报系统, 后者通过关联和挖掘, 不断拓展线索的边界, 输出大量与已知线索存在关联的新线索。利用威胁情报“一键溯源”(自动化追踪溯源), 是近年来学术界和工业界研究的热点。

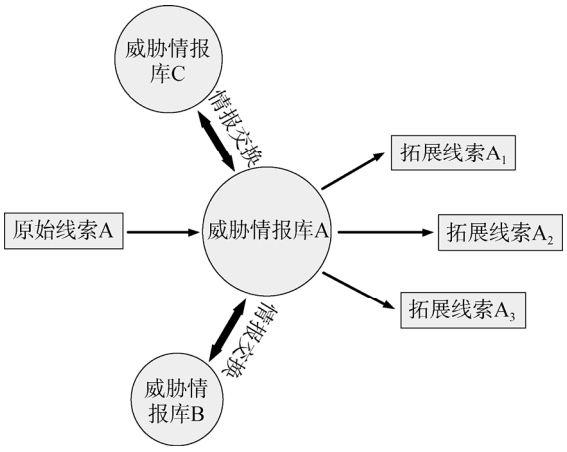


图 2 威胁情报追踪溯源原理

Figure 2 Attribution with threat intelligence

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

3.3 Web 追踪技术

出于精准推送广告等商业目的, 一些网络服务商需要标识浏览器用户, 从而产生了 Web 追踪技术。基于浏览器及插件存储机制(如 Cookie)的 Web 追踪, 是该领域最早使用也是最广为人知的技术, 代表性成果如 Cookie 同步[49]和 evercookies[49]。随着前端技术的发展, 以及浏览器厂商和 Web 开发者对用户隐私的重视, 基于浏览器及插件存储的追踪技术不再受到青睐, 新的 Web 追踪机制应运而生。

2010 年, Eckersley 等[50]最早提出在浏览器端采集一系列属性作为区分浏览器个体的指纹(原理如图 3)。该指纹碰撞率低且具有稳定性, 只随浏览器个体变化, 与浏览器内核和品牌无关, 可以用来跨网站追踪用户。近年来, 还有研究提出使用 Canvas 指纹[51]、CSS 指纹[52]跨网站追踪浏览器用户。Liu 等[53]和 KANG 等[54]还分别在前人研究基础上提出了抗干扰指纹生成算法, 增强了浏览器指纹的稳定性。此外, 还有研究基于操作系统、设备硬件或设备电池状态的指纹[55-57], 用于跨浏览器追踪用户; 基于机器学习、浏览器扩展或超声波计算指纹[58-60], 用于跨设备追踪用户。2015 年, Bujlow 等[61]系统性地综述了已有的 Web 追踪技术。除追踪外, 还有学者研究了如何利用浏览器特性获取用户隐私信息: 2015 年, 研究人员 diafygi 就在 github 上公开了基于 WebRTC 特性得到用户内外网 IP 地址的方法[62]; Rio Hosoi 等人[63]在此基础上构建了一个浏览器扫描系统, 可以探测用户所在内网的拓扑结构、主机操作系统以及域名解析等信息。Yan Zhu 还提出利用浏览器的 HSTS 和 CSP 机制嗅探用户访问过的域名, 以近似获取用户的浏览记录[64]。

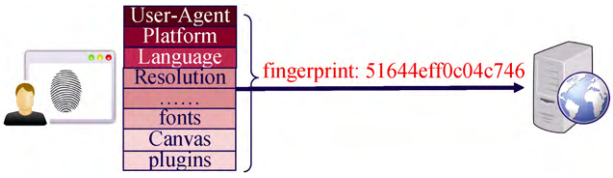


图 3 浏览器指纹原理

Figuer 3 Browser fingerprint

Web 在定向网络攻击中扮演着重要角色, 不仅是攻击者探测社工信息的重要平台, 还是投递攻击载荷的重要通道。浏览器指纹在溯源方面的一个重要应用场景便是跨网站追踪: 如图 4 所示, 攻击者同时拥有一个已公开的白身份和一个未公开的黑身份, 虽然两个身份访问了不同的网站, 但可以提取到相同的浏览器指纹, 这就可以通过指纹关联来溯源攻击者的真实身份(白身份)。

图 4 基于浏览器指纹跨网站追踪溯源原理

Figure 4 Attribution based on browser fingerprint in crossing websites scene

3.4 网络欺骗技术

网络欺骗技术(Cyber Deception)由蜜罐技术演化而来。传统蜜罐的仿真性和交互性较低, 容易被识别, 难以直接用于研究定向网络攻击的追踪溯源; 在对抗定向网络攻击的过程中, 防御者也逐渐意识到定向网络攻击难以避免, 继而开始考虑如何在这一前提下应对正在进行的攻击。Gartner 将网络欺骗技术定义为: 使用骗局或者假动作来阻挠或者推翻攻击者的认知过程, 扰乱攻击者的自动化工具, 延迟或阻断攻击者的活动, 通过使用虚假的响应、有意的混淆、以及假动作、误导等伪造信息达到“欺骗”的目的[65]。刘宝旭等[66-68]是国内研究网络欺骗的先驱, 他们最早于 2002 年就基于蜜罐技术提出了“陷阱防御”思路, 用于发现网络攻击和溯源取证; 2017 年, 国内的贾召鹏等[69]则系统地综述了网络欺骗技术。

网络欺骗技术主要包括欺骗环境构建和蜜饵部署。欺骗环境构建依赖于虚拟化技术和蜜罐技术, 前者主要目的是模拟真实内网, 构建一个包括主机和网络拓扑的高仿真欺骗基础环境; 后者则是在欺骗环境中部署包括大量泛业务的应用级蜜罐群。蜜饵部署主要是在可能的攻击路径上放置虚假的诱骗信息, 如代码注释、数字证书、Robots 文件、管理员密码、SSH 秘钥、VPN 秘钥、邮箱口令、ARP 记录、DNS 记录等, 从而诱使攻击者进入可控的欺骗环境。网络欺骗技术在定向网络攻击追踪溯源方面的作用可归纳为以下三个方面:

第一, 发现网络攻击, 此为追踪溯源的前提。网络欺骗通过部署虚假环境和蜜饵, 吸引和误导攻击者, 一旦这些正常用户难以触及的资源被访问, 则表明网络极有可能正在被攻击。2013 年, Jules 等[70]基于欺骗思想, 提出了 Honeywords 密码保护方案: 在口令文件中额外增加(N-1)个虚假的身份凭据, 如

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

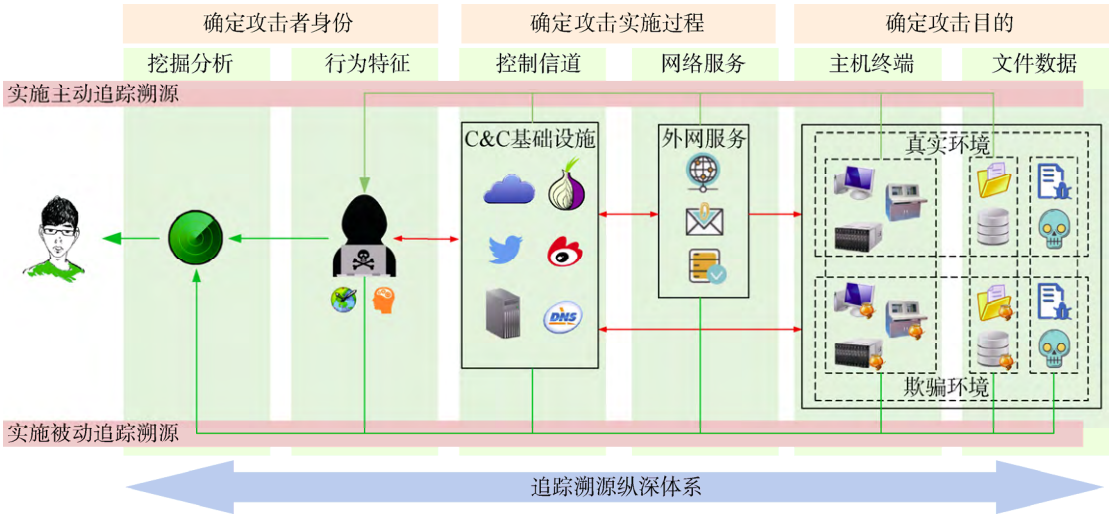


图 5 定向网络攻击追踪溯源层次化模型

Figure 5 Hierarchical model of targeted cyber attacks attribution

果攻击者使用了任意一个虚假口令，系统会立即感知到网络攻击。

第二，粘住网络攻击，为溯源网络攻击赢得时间和机会。防御者通过欺骗手段将网络攻击逐步吸引至虚假的欺骗环境，可以消耗攻击者的时间、精力和资源，减少其攻击重要真实系统的可能，还能够大量暴露其 TTP，从而为制定针对性的防御策略，乃至溯源反制赢得主动。2017 年，Brown Farinholt 等[71]通过详实的实验记录，论证了 RAT(Remote Access Trojan，远程控制木马)蜜罐作为陷阱防御手段，消耗攻击者精力和资源、防止其攻击真实系统的可行性。

第三，威慑网络攻击，其核心能力是追踪溯源。如果攻击者意识到已落入欺骗陷阱，这本身对其就是一种巨大的心理威慑：攻击行为已被发现，溯源线索可能已经暴露。此外，攻击者长期处于欺骗环境的监视之下，防御者有充足的时间和空间部署工具、设置机关，开展网络攻击追踪溯源工作，从而形成反制和威慑。

4 定向网络攻击追踪溯源层次化模型

定向网络攻击追踪溯源层次化模型，由网络服务、主机终端、文件数据、控制信道、行为特征和挖掘分析六个层次组成，本章详细阐述各层次的内涵及主要技术手段，并基于该模型提出建立纵深化追踪溯源体系，模型整体结构如图 5 所示。

4.1 网络服务层次

网络服务是信息系统内部和外部数据交换的通道，在定向网络攻击中扮演着重要角色：作为收集攻击目标情报的平台；作为第一跳攻击的目标；作为攻击载荷投递的通道，如“水坑攻击”(Watering Hole)[72]和“鱼叉式网络钓鱼”(Spear Phishing)[73]。因此在该层次上，可以相应地使用主被动结合的方法，从欺骗诱捕、标记取情两个方面追踪溯源定向网络攻击。

基于网络欺骗技术诱捕定向网络攻击。在网站等公开服务上，故意留下虚假信息(即面包屑)，以干扰攻击者收集信息的过程，改变其攻击路径。面包屑的作用有两点：作为防御陷阱发现网络攻击；将定向网络攻击吸引至特定的溯源环境实施诱捕反制。面包屑可以是虚假的邮箱地址、具备 Web 追踪能力的管理员登陆页面、虚假的账号口令等等。为了不引起攻击者怀疑，这些信息还要施以社会工程学手段作为伪装，例如将虚假的账号口令故意留在数据库备份文件中以增加迷惑性。除使用面包屑外，还可以部署多类型虚假的欺骗服务(如 Web，SSH，FTP)，吸引定向网络攻击。为了不被攻击者轻易识别，这些欺骗服务有别于传统蜜罐，不单单是网络流量层面的模拟，而是实际业务的“影子镜像”：以实际业务为蓝本进行构建，并做数据脱敏处理。

基于标记取情来追踪溯源定向网络攻击。前文提到的跨网站、跨浏览器、跨设备的 Web 用户追踪技术，是一种主动追踪溯源的方法，能够在汇聚多来源 Web 访问信息的基础上揭示攻击者的身份信息或溯源线索。一个典型的应用场景是，在被攻击网站提取攻击者的浏览器指纹，将其同其他网站上提取到的指纹比对，辨别攻击者在其他网站上的账号和身份，实现攻击者“黑白身份”的关联。在发现定向网络攻击的基础上，还可以考虑从攻击者一侧主动获取溯源线索。除直接利用漏洞反向渗透外，还可以

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

考虑利用软件和服务的特性获取溯源线索。例如在网站中嵌入 JavaScript 脚本, 利用浏览器特性获取攻击者的内外网 IP 地址、历史记录、所在时区等溯源线索; 回复鱼叉式钓鱼邮件并嵌入带有追踪功能的图片, 利用邮件客户端特性获取攻击者 IP 地址。基于漏洞和隐私追踪溯源攻击者, 会涉及法律和道德问题, 将后续章节中讨论。

4.2 主机终端层次

定向网络攻击中, 主机终端既包括攻击者使用的跳板资源也包括攻击目标。前者是攻击者直接掌握的资源, 一般会存有诸如登陆账号、远程连接信息等重要溯源线索; 后者则是攻击集中暴露的场所, 可以大量捕获攻击资源、流量和样本。因此, 在主机终端上的追踪溯源有着非常重要的意义。

跳板攻击主机上的追踪溯源可以使用技术手段和协调手段。所谓技术手段是指通过漏洞利用、弱口令等攻击方法, 在非配合情况下远程渗透跳板主机获取追踪溯源线索, 这是“以其人之道, 还治其人之身”的方法。技术手段技术虽然难度大, 但预期效果将十分明显。协调手段则一般是请求攻击主机的网络运营商或上级管理部门予以协助, 在他们的授权和支持下合理合法地取证调查。但是从实践来看, 商业公司和主管部门出于用户隐私保护的考虑, 一般会非常谨慎地对待协调取证请求。Mandiant 公司曾在其研究报告中将攻击者与跳板主机在远程桌面(Remote Desktop)连接中所使用的 IP 地理位置和键盘布局作为溯源证据[12], 这表明 Mandiant 公司已经能够在跳板主机上溯源取证。

防御者一侧的主机终端上的追踪溯源, 可以借鉴网络欺骗技术思路。典型的做法是: 首先, 在内网中部署大量虚假主机, 并故意预置漏洞和部署面包屑, 其目的是吸引网络攻击; 其次, 为了不引起攻击者察觉, 使其相信确实已攻击成功, 虚假主机的交互性要高, 如部署一定数量的文档或者模拟用户行为。这种欺骗诱捕的方法不仅有助于溯源网络攻击的目标和路径, 还可能获得追踪溯源攻击者身份的线索: 攻击者在同虚假主机的 Windows 远程桌面连接中, 有可能暴露键盘布局、剪贴板数据、磁盘目录、打印机名称等线索。图 6 展示了以色列 illusive network 公司的 Deception Everywhere 产品[74], 该产品是基于网络欺骗构建虚实结合内网环境的典型代表。该产品通过在内网中部署主机、服务器和网络设备等欺骗环境来误导攻击者, 使其无法做出正确判断, 并能实时跟踪攻击者的动作和行动路径。在学术界, Brown Farinholt 等[71]在研究 DarkComet 远程木马的工作中, 构造了 8 个高交互蜜罐主机, 用于模仿不同职业的用户(如游戏玩家、医生、政客等), 在 2 个星期内共计捕获到 785 次实时控制, 总时长达到 52.9 小时。文章在学术界首次详细分析了 RAT 控制者的行为。

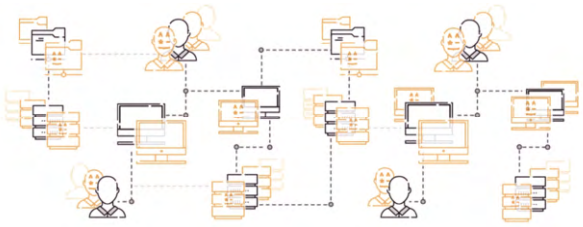


图 6 Deception Everywhere 构造虚假网络拓扑[74]

Figure 6 Deception network topology in Deception Everywhere[74]

4.3 文件数据层次

文件数据层次上的追踪溯源, 可以从被动分析恶意样本和主动施放诱饵文档两个方面展开。

恶意样本分析的主要目的是寻找样本中包含的可能与攻击者身份产生关联的溯源线索, 如变量命名、代码注释、编译路径、编译时间、拼写错误、高频字符串、典型算法、字体、俚语等等。从恶意样本中提取关键溯源线索的案例屡见不鲜: Careto 的代码中含有大量西班牙语元素[75]; Dukes 的大部分模块的错误提示是俄语[76]; Project Sauron APT 的配置文档中有很多意大利词汇[29]; Sanny APT 的钓鱼文档虽然通篇是俄语, 却使用了韩语特有的字体[77]; 白象 APT 的恶意样本含有疑似梵语的单词 Kanishk [78]。恶意样本分析从技术上可以分为静态分析和动态分析两类。静态分析不运行样本, 只是按文件格式分析提取样本中硬编码字符和特征属性等, 或者通过 API 调用推测样本的行为序列。为了对抗分析, 有些恶意样本会采用加壳、加密等手段保护自己, 这就需要采用动态分析的方法。动态分析一般会在虚拟机、沙箱等封闭隔离的模拟环境中运行样本, 从而提取动态出现的字符串并观察样本的行为。

主动施放文档诱饵利用了攻击者急于窃取文件数据这一心理, 是网络欺骗的思路。在蜜饵文档中嵌入漏洞利用代码是主动追踪溯源的好办法, 但是容易被攻击者检测。相比之下, 利用文档解释器的特性来追踪溯源则更容易躲避攻击者的防备。美国联邦调查局(Central Intelligence Agency, CIA)的“涂鸦”(Scribbles)项目[79]就利用了 Office 特性追踪溯源。“涂鸦”工具能为 Office 电子文档打上追踪水印(Watermark), 如果文档被打开, 水印就会主动向外

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

发送消息, 不仅可以预警文件已失窃, 还能够获得打开文档的主机 IP 地址等溯源线索。此外, 还出现了通过纸制实体文件追踪溯源窃密者的方法——打印机黄点(DocuColor Tracking Dot)[80]。这是一种暗记, 本质是在彩色激光打印机印刷的文件中嵌入隐蔽的黄点标记, 这些黄点肉眼无法识别, 其排列代表了特定的信息(打印时间和打印机编号, 原理如图 7 所示), 并且打印文件经扫描后生成的电子文档, 依然携带黄点信息。

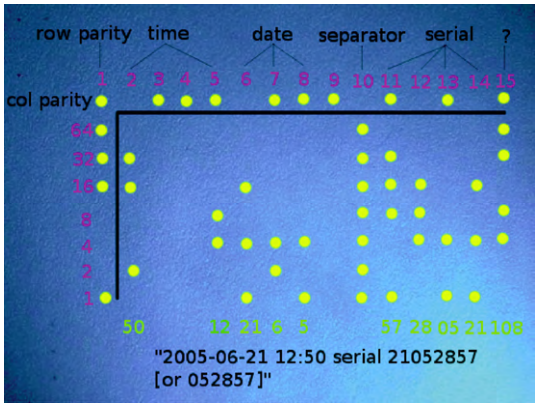


图 7 打印机黄点追踪解码示意图[80]

Figure 7 DocuColor tracking dot decoding[80]

4.4 控制信道层次

“控制信道”即“控制命令信道”(command and control channel, C&C), 这一术语源自僵尸网络, 攻击者可以通过 C&C 一对多地控制非合作用户终端[81]。定向网络攻击的控制命令信道在技术上更加先进、复杂和隐蔽。APT29 的攻击者就使用了域名前移(Domain Fronting)技术[82]非法利用知名网站进行隐蔽通信。控制信道层次的追踪溯源, 主要是从域名、服务器、网络账号等通信基础设施入手, 获取攻击者在注册、使用过程中留下的溯源线索。

域名一直备受追踪溯源人员关注, FireEye 公司曾把 DNS 注册信息列为七大线索之一[77]。域名的 whois 信息可能含有攻击者身份信息, 域名名字本身可能和攻击者的网络 ID 或者某种偏好产生关联, 在使用中也可能会泄露攻击者所属时区。一些攻击者为了躲避黑名单等常规检测措施, 会经常注册新域名, 这为追踪溯源提供了更多机会。Project CameraShy 报告追踪溯源的突破口便是攻击者一直使用的域名[15]。FireEye 公司曾指出即便是一些攻击者使用完全虚假的信息注册域名也会留下蛛丝马迹: 同一攻击者会在注册的多个域名之间共享相同的虚假信息, 并且构造的虚假信息可能与其文化背景产生关联[77]。

C&C 服务器的 IP 地址是相对容易获得的信息, 由 IP 地址也能容易地查询到对应的地理位置。但是, 某些 C&C 服务器会使用动态 IP 地址增强隐蔽性。动态 IP 的地理位置可以在较大范围内变化, 这种情况考虑使用“上级出口定位法”, 核心思想是: 即便是动态 IP 地址, 其邻近的上若干跳地址也不太容易变化, 并且路由路径末端相邻两跳节点的地理位置一般相近。

网络账号能够为追踪溯源提供关键线索。攻击者在建立控制信道过程中需要注册账号: 一是申请服务器和域名; 二是注册 Web2.0 服务(如推特、脸谱、微博等)用作 C&C[81]。最直接的获取网络账号溯源线索的方法是请求服务商协助, 但出于用户隐私的考虑, 服务商很难积极配合。因此利用服务特性获得注册用户信息就成为了比较可行的思路: 社交网络一般会公开用户的部分资料、地理位置等, “密码找回”功能也可能会暴露注册者的某些重要信息。

匿名网络也常被定向网络攻击者用作跳板网络或是控制信道, 因而对匿名通信系统的反向追踪具有重要意义, 主动流水印技术则可以部分解决这方面的问题。陈周国等[40]将流水印技术描述为“通过对匿名网络中传输数据进行调制处理, 将诸如水印等标识信息嵌入匿名网络数据中, 在接收端解调处理, 获取水印标识信息, 以此确认网络数据流关系”。姜建国等[33]和陈周国等[40]还对于匿名网络场景下的追踪溯源问题做了详细的综述。由于涉及复杂的技术原理, 本文不展开介绍。

4.5 行为特征层次

行为特征是攻击者作为自然人的正常表现, 是在生活和工作中长期养成的习惯, 非常难以改变。因此行为特征可以成为有力的溯源证据。典型的行为特征包括利益相关性、TTP 特征、作息规律等。

“利益相关性”是 APT 报告中经常提及的溯源线索, 是指从定向网络攻击形成的结果和危害反向推理攻击者身份。2015 年, 乌克兰电网遭到网络攻击, 造成大面积断电。考虑到当时乌克兰和俄罗斯两国的利益关系, 安全界就有推测认为此次攻击是俄罗斯黑客所为。利益相关性可以为追踪溯源提供大致的方向, 但容易抵赖, 比较适合作为辅助证据。此外, 本文认为一些报告中提及的“地缘政治”[4]概念, 其本质上是利益相关性。

攻击者的 TTP 特征, 也常被用作溯源线索。TTP 特征主要指攻击者使用的漏洞、工具和方法与已知的个人或组织高度相似, 或者惯用带有特定文化背景的网络服务。“方程式组织”(Equation Group)就因

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

其对使用加密算法和混淆策略情有独钟而得名。卡巴斯基还指出了若干条“方程式组织”的行为特征: 物理拦截邮寄的物品并植入木马程序; 将目标主机某一特征字符串的数千次哈希运算结果作为加密攻击载荷的密码[22]。后来结合一些泄密资料, 安全界揭开了“方程式组织”的真实身份[25-27]。

攻击者的作息规律同样是重要的溯源依据。作息规律是攻击者长期生活状态的反映, 想刻意掩饰比较困难。APT28 报告中指出 89%的恶意样本的编译时间恰为东四时区的工作时间(如图 8 所示), 进而推测 APT28 可能和俄罗斯有关[13]。白象 APT 报告和美人鱼 APT 报告也将攻击者作息规律作为溯源攻击组织的辅助证据[78, 83]。

4.6 挖掘分析层次

挖掘分析是追踪溯源攻击者身份最为重要的环节: 基于已获取的关键线索, 以威胁情报等为信息储备, 利用大数据、人工智能等技术手段, 排除干扰、关联线索, 实现溯源线索向攻击者身份的映射。

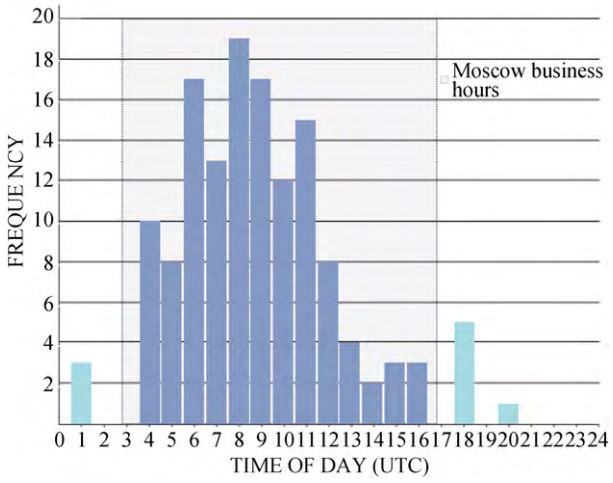


图 8 APT28 恶意样本编译时间分析(UTC 时间)[13]

Figure 8 Analysis of compile time of APT28 malicious samples (UTC) [13]

在白象 APT 的分析过程中, 溯源人员就综合已掌握的线索(如恶意样本中提取的系统账号), 基于互联网公开信息, 对白象组织的成员进行了全面的追踪溯源, 不但确定攻击者是一个由 10~16 人的组成的攻击小组, 还确定了主要参与成员的真实身份, 包括其姓名、联系方式、工作经历等高度敏感的个人信息[78, 84]。这是一次典型的利用威胁情报、搜索引擎和人工大数据分析来挖掘攻击者身份的过程。目前挖掘分析层次上的追踪溯源工作, 主要在以下三个方面:

第一, 威胁情报库的建设。广泛意义上的威胁情报应当尽可能广泛地包含有价值的情报, 不仅有漏洞库、社工库、样本库、黑客档案这类与攻防紧密相关的情报, 还应当把搜索引擎、社交网络、论坛新闻等都纳入其中。

第二, 挖掘分析的自动化。目前公开较有影响力的 APT 报告, 都使用到了挖掘分析的追踪溯源手段, 但自动化程度普遍较低。Project CameraShy 报告[15]就曾透露他们的分析挖掘过程主要依赖人工参与。自动化分析挖掘取代人工分析挖掘, 是当前研究热点也是未来趋势。

第三, 探索新的挖掘分析手段。这方面要解决的问题包括识别追踪溯源可利用的线索, 以及线索的运用。学术界在这方面做了一些前沿探索: 2017 年, Blond 等[86]提出使用机器学习的方法, 对 VirusTotal 网站[45]的用户身份进行分类。该方法只依赖上传恶意样本用户的基本信息, 不需要静态或动态分析恶意样本, 就可以有效区分攻击者和其他用户角色(受害者和第三方组织)。

4.7 纵深化体系

定向网络攻击的追踪溯源是一个复杂过程, 需要各层次相互配合, 建立纵深化的追踪溯源体系, 多维度追踪溯源定向网络攻击。定向网络攻击追踪溯源层次化模型的纵深性表现在两个方面: 从每个层次来看, 各层次都针对定向网络攻击的某个重要环节或关键资源, 可以概括为“溯源无处不在”; 从整体来看, 六个层次以“欺骗环境构建”、“多源线索提取”、“线索分析挖掘”为主线, 紧密耦合形成一个整体。具体来讲:

第一, 基于网络欺骗技术, 构建有利于追踪溯源的环境。在“网络服务”和“主机终端”层次上, 通过构建虚假的欺骗环境吸引网络攻击, 并将攻击者的精力和资源暴露、消耗于此, 不仅可以保护真实系统免受攻击, 也为确定攻击目的和实施过程, 以及提取攻击者身份关键线索创造了条件。

第二, 采用主被动结合的方法, 多源提取追踪溯源关键信息。“网络服务”、“主机终端”、“文件数据”、“控制信道”、“行为特征”五个层次, 面向定向网络攻击的各资源和环节获取追踪溯源关键线索, 且各有侧重: 前三个层次面向攻击路径上三个重要节点——外网服务、内网主机、重要数据或设施; “控制信道”层次面向攻击必需的通信资源; “行为特征”层次则面向攻击者本身的固有属性。在技术上, 既有诸如日志记录和样本分析的被动方法, 也有基于网络欺骗技术、在攻防两端获取线索的主动方法。

第三, 引入数据挖掘分析手段, 利用已知溯源

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

线索求解未知身份。防御者能够获取的溯源关键线索有限, 但是网络空间里公开的、私有的信息是海量的, “ 挖掘分析 ” 层次在二者之间架起了桥梁: 基于各层次提取到的关键线索, 利用挖掘分析方法, 在网络空间中不断拓展线索, 溯源攻击者身份。

5 定向网络攻击追踪溯源层次化模型评价

本章将尝试从洛克希德-马丁公司提出的 “ 网络入侵杀伤链 ” 模型[31]、FireEye 公司提出的 “ APT 溯源七大线索 ” [77]、本文提出的 “ 定向网络攻击追踪溯源三级目标 ”、实际追踪溯源案例四个角度, 评价定向网络攻击追踪溯源层次化模型的有效性。

5.1 从 “ 网络入侵杀伤链 ” 模型角度的评价

“ 网络入侵杀伤链 ” (Intrusion Kill Chain)模型, 用于描述网络入侵的过程。该模型将入侵过程分为目标侦查(Reconnaissance)、武器生产(Weaponization)、载荷投递(Delivery)、突防利用(Exploitation)、安装植入(Installation)、命令控制(Command and Control)、任务执行(Actions on Objectives)七个步骤。本节将结合攻击模型, 分析追踪溯源模型的有效性。

在目标侦查和武器生产阶段, 可以在 “ 网络服务 ” 和 “ 主机终端 ” 层次上予以应对。防御者通过部署面包屑以及虚假的网络服务和主机终端, 致使攻击者获得不正确的情报, 甚至误导其锁定错误的攻击目标、生产不恰当的网络武器。

载荷投递、突防利用和安装植入, 是紧密相关的三个阶段。在 “ 网络服务 ”、“ 主机终端 ” 和 “ 文件数据 ” 层次上, 有以下三种对抗方式: 其一, 构造欺骗环境粘住网络攻击, 目的是尽可能多地捕获恶意代码样本和暴露攻击手段, 增加获取追踪溯源线索的可能性; 其二, 被动手段提取溯源线索, 如记录流量和日志、分析恶意样本等; 其三, 在攻击者一侧以主动方式提取追踪溯源线索, 如使用浏览器追踪脚本、追踪邮件等等。

在命令控制阶段, 攻击者必定要用到通信基础设施, 如域名、C&C 服务器、网络账号。在 “ 控制信道 ”层次上, 溯源人员主要通过查询和关联的方法, 提取溯源线索。

在任务执行阶段, 定向网络攻击的主要表现是破坏系统和窃取数据, 在 “ 网络服务 ”、“ 主机终端 ” 和 “ 文件数据 ” 层次上, 上述动作可以被部署的欺骗环境和蜜饵及时感知, 再结合利益相关性, 就可以对攻击者身份有一个大致的推测。同时, 也可以在蜜饵文档里植入漏洞利用或追踪代码, 主动溯源攻击者。

在 “ 载荷投递 ”、“ 突防利用 ”、“ 安装植入 ”、“ 命令控制 ” 和 “ 任务执行 ” 阶段, 攻击者都有可能表现出一定的行为特征, 如时区特征、惯用工具、常用技术技巧等, 在 “ 行为特征 ” 层次上关注和提取这些特征, 有机会获取到溯源关键线索。

在 “ 载荷投递 ”、“ 突防利用 ”、“ 安装植入 ” 和 “ 命令控制 ”阶段, 防御者都可能已经提取到若干追踪溯源线索, 在 “ 挖掘分析 ” 层次上将对这些线索做进一步利用, 以溯源攻击者身份。

综上, 本文提出的定向网络攻击追踪溯源层次化模型, 可以在 “ 网络入侵杀伤链 ” 模型所述的各个步骤中, 实施追踪溯源以应对定向网络攻击, 具体关系详见表 2。

5.2 从 APT 追踪溯源七大线索角度的评价

FireEye 公司在其参与的 1500 余宗追踪溯源工作的基础上, 归纳总结了七大溯源线索: 键盘布局(Keyboard Layout)、样本附加信息(Malware Metadata)、内嵌字体(Embedded Fonts)、DNS 注册信息(DNS Registration)、语言文字(Language)、远控工具管理配置(RAT Administration Tool Configuration)、行为模式(Behavior)。本节将结合上述七大溯源线索, 分析定向网络攻击追踪溯源层次化模型的有效性。

键盘布局反映了攻击者主机或编译器配置的默认语言和区域。该信息通常隐藏在电子邮件、远程桌面连接、可执行文件和文档文件中, 相应地可以在 “ 网络服务 ”、“ 主机终端 ” 和 “ 文件数据 ” 层次上应对。

恶意样本的二进制字节流中可能包含许多附加信息, 如属性、编译路径等, 通常暗示了攻击者的母语、地域甚至是昵称, 是追踪溯源的重要线索。“ 文件数据 ” 层次上的动静态分析可以提取这些信息。

内嵌字体可以反映攻击者的惯用语言, 在邮件和文档中比较常见, 可以用于辅助推断攻击者身份。例如 “ 宋体 ” 是中文用户惯用字体, “ Batang ” 则是韩语用户惯用字体。“ 网络服务 ” 和 “ 文件数据 ” 层次可以提取到内嵌字体线索, 例如鱼叉式钓鱼邮件的原始报文, PDF 或 Office 文档类型恶意样本等。

DNS 信息作为溯源线索由两部分组成: 从恶意样本中提取到的域名信息, 以及通过域名查询到的 DNS 注册信息。这两部分线索能够分别从 “ 文件数据 ” 和 “ 控制信道 ” 层次得到。

远控工具管理配置, 通常包含密码、C&C 地址、互斥量、任务名等, 这些信息在 “ 文件数据 ”层次上, 通过动静态分析远控工具的被控端有可能得到。

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

表 2 各层次与“网络入侵杀伤链”模型的关系

Table 2 Relationship between each attribution level and the Intrusion Kill Chain Model

层次	网络服务	主机终端	文件数据	控制信道	行为特征	挖掘分析
目标侦查	√	√				
武器生产	√	√				
载荷投递	√	√	√		√	√
突防利用	√	√	√		√	√
安装植入		√	√		√	√
命令控制				√	√	√
任务执行	√	√	√		√	

表 3 各层次与追踪溯源七大线索的关系

Table 3 Relationship between proposed attribution levels and seven key attribution clues

层次	网络服务	主机终端	文件数据	控制信道	行为特征	挖掘分析
键盘布局	√	√	√			
样本附加信息			√			
内嵌字体	√		√			
DNS 信息			√	√		
语言文字	√		√	√		
远控管理配置		√	√			
行为模式					√	

行为模式线索揭示了攻击者的作案动机和技术特点, 这与本文所述的“行为特征”层次追踪溯源不谋而合。

综上, 本文提出的定向网络攻击追踪溯源层次化模型, 在相应层次上能够有效获取追踪溯源关键线索, 具体关系详见表 3。

5.3 从定向网络攻击追踪溯源三级目标角度的评价

本文提出了定向网络攻击追踪溯源的三级目标: 确定攻击目的、实施过程和攻击者身份。

定向网络攻击通常以窃密和破坏系统为目的, 因此在“网络服务”、“主机终端”和“文件数据”三个层次上, 可以通过部署欺骗资源来诱骗攻击者暴露其攻击目的, 从而满足追踪溯源的第一级目标。

在“网络服务”和“主机终端”层次上, 通过主动构建欺骗环境以及被动记录日志流量等手段, 可以有效描绘定向网络攻击的参与资源和行动路径, 从而完成第二级目标的追踪溯源。

定向网络攻击追踪溯源层次化模型的前五个层次, 都具备获取攻击者关键线索的能力, “挖掘分析”则是对既有溯源线索的深层次利用, 六个层次相互配合完成攻击者身份的溯源。

综上, 本文提出的定向网络攻击追踪溯源层次化模型, 较好地契合了定向网络攻击的三级目标, 具体关系参见表 4。

5.4 从实际案例角度的评价

本文在阐述各追踪溯源层次时, 已经分别引用大量溯源案例作为佐证, 说明各层次在实际的定向网络攻击追踪溯源工作中的作用。本节将具体引用白象 APT 这一典型的追踪溯源案例, 评价所提出的定向网络攻击追踪溯源层次化模型。

表 4 各层次与追踪溯源三级目标的关系

Table 4 Relationship between proposed attribution levels proposed attribution goals

层次	第一级目标	第二级目标	第三级目标
网络服务	√	√	√
主机终端	√	√	√
文件数据	√		√
控制信道			√
行为特征			√
挖掘分析			√

安天公司曾于 2016 年和 2017 年两次发布研究报告, 披露白象组织(WhiteElephant)的活动[78, 84], 360 追日团队也发布过针对该组织的研究报告, 并将其命名为“摩诃草”[85]。白象 APT 是已公开的较为成功的追踪溯源案例, 溯源人员掌握了攻击者的攻击目的、实施过程, 以及主要成员的真实身份。本文在此不讨论溯源结论的真实性, 仅做技术性分析。

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

表 5 白象 APT 追踪溯源证据和各追踪溯源层次的对应关系

Table 5 Relationship between evidences of the WhiteElephant APT and proposed attribution levels

层次	追踪溯源线索与方法
网络服务	通过相同的邮箱地址关联该组织的多次攻击
主机终端	在被攻击主机上提取到数千个恶意样本
文件数据	从恶意样本中提取到攻击者系统账号、样本编译时间等, 其中一条账号线索暗示了攻击者的文化背景 从 iOS 恶意样本中提取到开发者信息 通过恶意样本包含的编译路径等静态字符串关联该组织的多次攻击
控制信道	C&C 域名的大量注册信息 通过共用的 C&C 域名关联该组织的多次攻击
行为特征	攻击目标符合利益相关性 工作时间具有明显的时区特征
挖掘分析	基于互联网公开信息, 刻画攻击者画像 精确溯源了一名主要成员的身份信息

在“网络服务”层次上, 溯源人员通过提取攻击者惯用的多个邮箱, 关联了该组织不在同时间内发动的多次攻击, 极大地丰富了溯源线索。

在“主机终端”层次上, 溯源人员在被攻击主机上提取到了数千个恶意样本, 这些样本中包含了大量与攻击者身份关联的溯源线索, 为后续溯源工作的突破奠定了基础。

在“文件数据”层次上, 攻击者在恶意样本中留下了大量的溯源线索: Windows 恶意样本中包含大量的样本编译时间、编程人员的账号等重要线索, 并且其中一条账号线索直接暗示了攻击者的文化背景; 某个 iOS 样本中含有真实的开发者信息; 样本中含有可以将多次攻击关联起来的单词拼写错误。

在“控制信道”层次上, 攻击者不慎留下了多个 C&C 域名的注册信息, 这些信息不仅提供了攻击者的身份线索, 还被溯源人员用于关联多次攻击。

在“行为特征”层次上, 溯源人员分析了攻击目标的利益相关性以及恶意样本编译时间的时区特征, 分析结论共同暗示了白象组织背后的支持者。

在“挖掘分析”层次上, 溯源人员则以所掌握的特征用户名为突破口, 结合互联网上公开的信息, 确定了白象组织的规模和成员, 并详细溯源了其中一位主要成员的真实身份, 包括其真实姓名、学习工作经历、项目经历、组织背景等等。

综上, 白象 APT 的追踪溯源案例, 较好地印证了本文提出的定向网络攻击追踪溯源层次化模型的技术可行性有效性(参见表 5)。

6 讨论

6.1 法律与道德问题

使用入侵渗透或者获取用户隐私的手段追踪溯源网络攻击, 可能会涉及法律和道德问题, 并且又因定向网络攻击常用于国家间或组织间网络对抗而增加了这一问题的复杂性: 第一, 在追踪溯源过程中入侵渗透必要的网络设施、获取必要的用户隐私, 这种行为是否合法、获得的证据是否有效; 第二, 如果上述行为被允许, 那么谁将被赋予这样的权力, 第三方公司和机构(如 ISP、CERT 组织、网络服务商)是否需要配合; 第三, 上述两点如何获得国际上的认同与协作。

APT1 报告就有多处涉嫌侵犯用户隐私: 溯源人员获知了攻击者在 Gmail、Facebook、rootkit 等网站注册账号的隐私信息, 获得了大量的攻击者使用的密码, 甚至掌握了攻击者部分邮箱的邮件内容。从 2014 年 5 月美国司法部决定起诉可能参与 APT1 的五名中国军官[87, 88]这一事实来看, 可以认为美国司法机构认可了证据的有效性, 但这却遭到了中国政府的强烈抗议[89]。

追踪溯源过程中面临的法律与道德问题目前还难有定论, 但是“网络空间主权”为解决这一问题指明了非常好的方向。方滨兴主编的《论网络空间主权》[11]著作, 详细诠释了网络空间主权的概念、内涵与外延。文献给出了网络空间主权的定义, 明确了网络空间管辖权和自卫权, 即“网络空间的构成设备、承载数据及其操作受所属国的司法与行政管辖”, “国家拥有保护本国网络空间不被侵犯及保持相应军事能力的权利”, 同时还指出网络空间主权应该具有“尊重主权、互不侵犯、互不干涉内政、主权平等”的四项基本原则。

因网络攻击追踪溯源而产生的法律与道德问题, 不是本文的主要研究内容。本文认为, 应当在网络空间主权的框架下, 以国内立法和国际公约的形式解决部分网络攻击追踪溯源技术手段面临的法律和道德问题。通过国内立法解决基于入侵渗透或获取用户隐私的追踪溯源手段的合法性、有效性, 以及权力执行机构的问题; 通过国际公约, 就上述两点问题达成国家间共识, 并寻求国际合作。

6.2 溯源线索的伪装问题

防御者在追踪溯源定向网络攻击的同时, 攻击者也在极力地做着反追踪溯源工作, 伪装溯源线索便是一种常见的方法。伪装溯源线索, 可能会扰乱溯源人员的判断, 把溯源工作引向错误的方向, 甚至

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

还有可能把网络攻击嫁祸给无辜的第三方。

攻击者一般基于自身对追踪溯源方法的认知伪装溯源线索。常用的方法包括使用跳板网络发动攻击, 使用虚假信息注册域名和账号, 恶意代码中尽量使用英语或非母语语言等等, 这些方法在实际的定向网络攻击案例中也都有印证。本文认为, 从理论和技术角度来看, 不存在不可伪装的溯源线索, 只是攻击者认知和成本代价的问题。溯源线索的伪装在网络攻击中客观存在且不可避免, 所以溯源信息的去伪存真是不可回避的问题。

识别攻击者伪装的溯源线索、找出基本的溯源证据可信支点, 是网络攻击追踪溯源需要研究的重要内容, 但不是本文要重点要讨论的内容。从本文提出的定向网络攻击追踪溯源层次化模型来看, “ 行为特征 ”层次上的追踪溯源, 最有可能成为解决上述问题的关键。第一, 利益相关性是攻击者难以伪装的一项指标。定向网络攻击是一项高成本的工作, 如果攻击者不能从中获得利益回报, 甚至让第三方“ 坐收渔利 ”, 那么就失去了它的意义。因此, 通过分析利益相关性, 即使不能明确追踪溯源, 也至少可以界定大致的追踪溯源范围。第二, 攻击者的行为特征是其在生活和工作中长期养成的习惯, 不仅难以改变, 还往往带有鲜明的地域和文化特征, 这些溯源线索难以伪装。

6.3 诱捕定向网络攻击的安全风险

本文提出在追踪溯源过程中引入网络欺骗思想, 构建虚实结合的网络和系统环境, 采用主被动相结合的方式, 诱捕定向网络攻击, 收集追踪溯源线索。

网络欺骗技术在更好地解决定向网络攻击追踪溯源问题的同时, 也可能引发新的安全风险: 不再是阻断网络攻击、拒网络攻击于内网之外, 而是主动将网络攻击诱骗到内网之中, 这似乎是给防御者以压力、给攻击者以 “ 便利 ”。虽然网络攻击被假设限制在欺骗环境之中, 但无法避免攻击者使用 0day、社工等高级手段突破欺骗环境, 使攻击蔓延至真正的内网。这不仅仅给目标网络带来巨大的安全风险, 由此而引发的责任划分问题也难以处理。

没有详细论述如何规避诱捕定向网络攻击可能带来的安全风险是本文工作的一处不足, 也是未来要重点研究解决的问题。但本文认为: 这是一个技术问题, 也是一个策略问题。从技术角度讲, 在欺骗环境的设计实现上, 可以通过先进的技术、灵活的思路, 最大化避免此类问题的发生; 从策略角度讲, 在 “ 定向网络攻击难以避免 ”这一大前提下, “ 拒敌于内网之外 ”和 “ 诱敌于欺骗环境之中 ”, 孰优孰劣还不能定论。

7 总结和未来工作

定向网络攻击对网络空间安全构成了极大的威胁, 如何有效应对定向网络攻击已成为学术界和工业界共同关注的问题。本文认为定向网络攻击难以避免, 单纯地依靠发现攻击、阻断攻击的被动防御方法, 难以有效应对现有的定向网络攻击威胁, 需要将追踪溯源作为威慑定向网络攻击的重要手段。本文的主要工作是定向网络攻击追踪溯源方面的理论研究, 从模型构建的角度出发, 开展了如下几方面的工作:

给出了定向网络攻击追踪溯源的形式化定义和分类, 并指出追踪溯源的三级目标: 确定网络攻击的目的, 确定网络攻击的实施过程, 确定攻击者的身份。

借鉴了网络欺骗等领域的研究成果, 提出将网络欺骗技术引入定向网络攻击追踪溯源, 构建虚实结合的网络和系统环境, 采用主被动相结合的方式, 追踪溯源定向网络攻击。

建立了以 “ 网络服务 ”、“ 主机终端 ”、“ 文件数据 ”、“ 控制信道 ”、“ 行为特征 ”、“ 挖掘分析 ” 六个层次为划分的定向网络攻击追踪溯源模型。

基于定向网络攻击追踪溯源层次化模型, 提出构建追踪溯源的纵深体系: 各层次都针对定向网络攻击某个重要环节或关键资源, 溯源无处不在; 六个层次以 “ 欺骗环境构建 ”、“ 多源线索提取 ”、“ 线索分析挖掘 ” 为主线, 紧密耦合形成一个整体。

从洛克希德-马丁公司提出的“ 网络入侵杀伤链 ” 模型、FireEye 公司提出的 “ APT 溯源七大线索 ” 以及本文提出的 “ 定向网络攻击追踪溯源三级目标 ” 三个方面, 评价了定向网络攻击追踪溯源层次化模型, 认为该模型能够较好地应对定向网络攻击追踪溯源问题。

本文还讨论了部分追踪溯源技术可能涉及的法律与道德问题, 攻击者故意伪装溯源线索问题, 以及诱捕定向网络攻击的安全风险。

基于上述内容, 提出定向网络攻击追踪溯源未来的几方面工作:

1) 面向追踪溯源的网络欺骗环境构建, 包括构建虚拟化的基础网络环境, 部署高仿真虚拟主机和服务, 施放多重蜜饵资源, 以及欺骗环境本身可靠性研究。

2) 主动追踪溯源技术方面的研究, 包括对现有技术的深入探讨, 以及新技术新策略的探索。

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

3) 基于已知追踪溯源线索自动化挖掘分析攻击者身份, 以及伪装线索的智能化识别。

4) 追踪溯源工作面临的法律道德问题研究, 以及国际合作方面的研究。

参考文献

[1] Aditya K Sood and Richard Enbody, “Targeted cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware,” National Defense Industry Press, 2016.
((美)Aditya K Sood 和 Richard Enbody 著. 孙宇军等译. 定向网络攻击——由漏洞利用与恶意软件驱动的多阶段攻击.国防工业出版社. 2016。)

[2] “Kaspersky Lab provides its insights on Stuxnet worm,” Kaspersky Lab., https://www.kaspersky.com/about/press-releases/2010_kaspersky-lab-provides-its-insights-on-stuxnet-worm, Sep. 2010.

[3] “Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack,” The Washington Post, Feb. 2011.

[4] “2016中国高级持续性威胁研究报告”, SkyEye and HeliosTeam, http://zhuiri.360.cn/upload/APT-2016.pdf, Feb. 2017.

[5] “Analysis of the Cyber Attack on the Ukrainian Power Grid”, E-ISAC, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, Mar. 2016.

[6] “Sednit adds two zero-day exploits using ‘Trump’s attack on Syria’ as a decoy,” ESET, https://www.welivesecurity.com/2017/05/09/sednit-adds-two-zero-day-exploits-using-trumps-attack-syria-decoy/, MAY. 2017.

[7] “Taiwan Presidential Election: A Case Study on Thematic Targeting,” PwC, http://pwc.blogs.com/cyber_security_updates/2016/03/taiwant-election-targetting.html#_ftn1, Mar. 2016.

[8] “Ukraine Election Narrowly Avoided ‘Wanton Destruction’ From Hackers,” The Christian Science Monitor, June 2014.

[9] Cai Guilin, Wang Baosheng, Wang Tianzuo, Luo Yuebin, Wang Xiaofeng and Cui Xinwu, “Research and development of moving target defense technology,” *Journal of Computer Research and Development*, vol. 53, no. 5, pp. 375-378 (in Chinese), 2016.
(蔡桂林, 王宝生, 王天佐, 罗跃斌, 王小峰, 崔新武, “移动目标防御技术研究进展”, *计算机研究与发展*, 2016, 53(5): 375-378。)

[10] Rui Zhuang, Su Zhang, Scott DeLoach, Xinming Ou, and Anoop Singhal, “Simulation-based approaches to studying effectiveness of moving-target network defense,” in Proc. National Symposium on Moving Target Research, pp. 1-12, 2012.

[11] 方滨兴主编, “论网络空间主权”, 科学出版社, 2017。

[12] “APT1: Exposing One of China's Cyber Espionage Units,” FireEye, Inc., https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf, February 18, 2013.

[13] “APT28: A Window into Russia's Cyber Espionage Operations,” FireEye, Inc., https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf, Oct. 2014.

[14] “APT28: AT THE CENTER OF THE STORM,” FireEye, Inc., https://www2.fireeye.com/WEB-2017-RPT-APT28.html?utm_source=FEcom&utm_campaign=intel-apt28&utm_medium=blog, Nov. 2017.

[15] “Project CameraShy: Closing the Aperture on China’s Unit 78020,” ThreatConnect Inc. and Defense Group Inc., http://www.threatconnect.com/camerashy/, 2015.

[16] “Obama Order Sped Up Wave of Cyberattacks Against Iran,” The New York Times Company, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=2&_r=1&seid=auto&smid=tw-nytimespolitics&pagewanted=all, Jun. 2012.

[17] “Duqu: A Stuxnet-like malware found in the wild,” Laboratory of Cryptography of Systems Security (CrySyS), http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf, Oct. 2011.

[18] “The ‘Red October’ Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies,” Kaspersky Lab., https://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation/, Mar. 2014.

[19] “Sandworm Team and the Ukrainian Power Authority Attacks,” FireEye, Inc., https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html, Jan. 2016.

[20] “Penquin’s Moonlit Maze: The Dawn of Nation-State Digital Espionage,” Kaspersky Lab., https://securelist.com/files/2017/04/Penquins_Moonlit_Maze_PDF_eng.pdf, Apr 2017.

[21] “THE DUQU 2.0 technical Details,” Kaspersky Lab., https://securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf, Jun. 2015.

[22] “Equation: The Death Star of Malware Galaxy,” Kaspersky Lab., https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/, Feb. 2015.

[23] “Edward Snowden,” Wikimedia Foundation, Inc., https://en. wikipedia.org/wiki/Edward_Snowden, Jan. 2018.

[24] “The Shadow Brokers,” Wikimedia Foundation, Inc., https://en.wikipedia.org/wiki/The_Shadow_Brokers, Nov. 2017.

[25] “Equation Group,” Wikimedia Foundation, Inc., https://en. wikipedia.org/wiki/Equation_Group, Nov. 2017.

[26] “THE NSA LEAK IS REAL, SNOWDEN DOCUMENTS CONFIRM,” theintercept.com, https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/, Aug. 2016.

[27] “Group claims to hack NSA-tied hackers, posts exploits as proof,” WIRED Media Group, https://arstechnica.com/information-technology/2016/08/group-claims-to-hack-nsa-tied-hackers-posts-exploits-as-proof/, Aug. 2016.

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

[28] “ProjectSauron: top level cyber-espionage platform covertly extracts encrypted government comms,” Kaspersky Lab., https:// securelist.com/faq-the-projectsauron-apt/75533/, Aug. 2016.

[29] “Strider: Cyberespionage group turns eye of Sauron on targets,” Symantec Corporation, https://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron-targets, Aug. 2016.

[30] David A. Wheeler and Gregory Noel Larsen, “Techniques for Cyber Attack Attribution,” Institute for Defense Analyses, Oct. 2003.

[31] E. M. Hutchins, M. J. Cloppert, R. M. Amin, “Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains”, *Leading Issues in Information Warfare & Security Research*, vol. 1, pp. 80-106, 2011.

[32] Chen Zhouguo, Pu Shi, Hao Yao and Huang Chen, “Levels Analysis of Network Attack Traceback,” Computer Systems & Applications, vol. 23, no. 1, pp. 1-7 (in Chinese), 2014.
(陈周国, 蒲石, 郝尧, 黄宸, “网络攻击追踪溯源层次分析”, *计算机系统应用*, 2014, 23(1):1-7。)

[33] Jiang Jianguo, Wang Jizhi, Kong Bin, Hu Bo and Liu Jiqiang, “On the Survey of Network Attack Source Traceback,” *Journal of Cyber Security*, vol. 3, no. 1, pp. 111-131 (in Chinese), 2018
(姜建国, 王继志, 孔斌, 胡波, 刘吉强, “网络攻击源追踪技术研究综述”, *信息安全学报*, 2018, 3(1):111-131。)

[34] Cohen D and Narayanaswamy K, “Attack Attribution in Non-Cooperative Networks,” in Proc. the Fifth Annual IEEE *SMC Information Assurance Workshop* (IAW 2004), pp. 436-437, 2004.

[35] Stone R, “CenterTrack: an IP overlay network for tracking DoS floods,” in Proc. the 9th USENIX Security Symposium (USENIX Security ’09), 2000.

[36] “ICMP Traceback message,” AT&T Labs Research and Nortel Networks, https://tools.ietf.org/html/draft-ietf-itrace-04, Feb. 2003.

[37] Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson, “Practical network support for IP traceback,” in Proc. ACM SIGCOMM *Computer Communication Review*, vol. 30, no. 4, pp. 295-306, 2000.

[38] Andrey Belenky and Nirwan Ansari, “IP traceback with deterministic packet Marking,” IEEE *Commun. Letters*, vol. 7, no. 4, pp. 162–164, 2003.

[39] Alex C. Snoeren, Craig Partridge, Luis A. Sanchez, Christine E. Jones, Fabrice Tchakountio, Stephen T. Kent and W. Timothy Strayer, “Hash-based IP traceback,” in Proc. ACM *SIGCOMM Computer Communication Review*, vol. 31, no. 4, pp. 3-14, 2001.

[40] Chen Zhouguo, Pu Shi, Shixiong Zhu, “Traceback technology for anonymous network,” *Journal of Computer Research & Development*, vol. 49, Suppl., pp.111-117 (in Chinese), 2012.
(陈周国, 蒲石, 祝世雄, “匿名网络追踪溯源综述”, *计算机研究与发展*, 2012, 49(Suppl.): 111-117。)

[41] “Definition: threat intelligence,” Gartner Inc., https://www.gartner.com/doc/2487216/definition-threat-intelligence, Oct. 2015.

[42] “The Pyramid of Pain”, David J. Bianco, http://rvasec.com/slides/2014/Bianco_Pyramid%20of%20Pain.pdf, 2014.

[43] Yang Zeming, Li Qiang, Liu Junrong, Liu Baoxu, “Research of Threat Intelligence Sharing and Using for Cyber Attack Attribution,” *Journal of Information Security Research*, vol. 1, no. 1, pp.31-36 (in Chinese), 2015.
(杨泽明, 李强, 刘俊荣, 刘宝旭, “面向攻击溯源的威胁情报共享利用研究”, *信息安全研究*, 2015, 1(1): 31-36。)

[44] “Threat Crowd,” ALIENVAULT, INC., https://www.threatcrowd.org/.

[45] “VirusTotal,” VirusTotal, https://www.virustotal.com/.

[46] “360 威胁情报中心”, 360 企业安全, https://ti.360.net/。

[47] “微步在线情报社区”, 北京微步在线科技有限公司, https://x.threatbook.cn/。

[48] “NOSEC 大数据安全协作平台, 威胁情报平台”, NOSEC 大数据安全协作平台, https://nosec.org/。

[49] Acar G., Eubank C., Englehardt S., Juarez M., Narayanan A., and Diaz C., “The web never forgets: Persistent tracking mechanisms in the wild,” in Proc. the 2014 ACM SIGSAC Conference on *Computer and Communications Security* (CCS’14), pp. 674-689, 2014.

[50] P. Eckersley, “How unique is your web browser?” in Proc. the 10th *International Conference on Privacy Enhancing Technologies* (PETS’10), pp. 1-18, 2010.

[51] K. Mowery and H. Shacham, “Pixel perfect: Fingerprinting canvas in HTML5,” in Proc. Web 2.0 *Security and Privacy* (W2SP 2012), pp. 1-12, 2012.

[52] Takei N., Saito T., Takasu K., and Yamada T, “Web browser fingerprinting using only cascading style sheets,” in Proc. the 10th International Conference on Broadband and Wireless Computing, *Communication and Applications* (BWCCA), pp. 57-63, 2015.

[53] Xiaofeng Liu, Qixu Liu, Xiaoxi Wang, and Zhaopeng Jia, “Fingerprinting Web Browser for Tracing Anonymous Web Attackers,” in Proc. *2016 IEEE First International Conference on Data Science in Cyberspace* (DSC), pp. 222-229, 2017.

[54] Kang Nianhua, Chen Mingzhi, Feng Yingyan, Liu Chuanbao, “An Anti-interference Browser Fingerprinting Generation Algorithm Based on Implicitly Acquiring Features,” *Netinfo Security*, vol. 17, no. 4, pp. 71-77. (in Chinese), 2017.
(康年华, 陈明志, 冯映燕, 刘川葆, “一种基于特征信息隐式获取的抗干扰浏览器指纹生成算法”, *信息网络安全*, 2017(4):71-77。)

[55] Nakibly G, Shelef G and Yudilevich S, “Hardware fingerprinting using HTML5,” *Computing Research Repository* (CoRR), vol. 3, pp. 1-5, 2015.

[56] Y. Cao, S. Li, and E. Wijmans, “(Cross-)Browser Fingerprinting via OS and Hardware Level Features,” in Proc. the 2017 *Network*

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

and Distributed System Security Symposium (NDSS 2017), 2017.

[57] Diaz C., Olejnik L., Acar G., and Casteluccia C., "The leaking battery: A privacy analysis of the html5 battery status api," *Lecture Notes in Computer Science*, vol. 9481, pp. 254-263, 2015.

[58] Díaz-Morales R., "Cross-device tracking: Matching devices and cookies," in Proc. 2015 IEEE *International Conference on Data Mining Workshop* (ICDMW), pp. 1699-1704, 2015.

[59] Starov O. and Nikiforakis N., "Xhound: Quantifying the fingerprintability of browser extensions," in Proc. 2017 *IEEE Symposium on Security and Privacy* (S&P), pp. 941-956, 2017.

[60] Mavroudis V., Hao S., Fratantonio Y., Maggi F., Kruegel C., and Vigna G., "On the privacy and security of the ultrasound ecosystem," in Proc. *Privacy Enhancing Technologies*, no. 2, pp. 95-112, 2017.

[61] Bujlow T., Carela-Español V., Sole-Pareta J., and Barlet-Ros P., "A survey on web tracking: Mechanisms, implications, and defenses," in Proc. the IEEE, vol. 105, no. 8, pp. 1476-1510, 2017.

[62] "webrtc-ips," https://github.com/diafygi/webrtc-ips, Jul. 2015

[63] Hosoi R., Saito T., Ishikawa T., Miyata D., and Chen Y., "A browser scanner: Collecting intranet information," in Proc. 2016 19th *International Conference on Network-Based Information Systems* (NBiS), pp. 140-145, 2016.

[64] "Weird New Tricks for Browser Fingerprinting," ToorCon 2015, https://zyan.scripts.mit.edu/presentations/toorcon2015.pdf, Jun. 2015.

[65] "Emerging Technology Analysis: Deception Techniques and Technologies Create Security Technology Business Opportunities," Gartner Inc., https://www.gartner.com/doc/3096017/emerging-technology-analysis-deception-techniques, Jul. 2015.

[66] 刘宝旭, 曹爱娟, 许榕生, "陷阱网络技术综述", *网络安全技术与应用*, 2003(1):65-69。

[67] Liu Baoxu and Xu Rongsheng, "Study and design of the proactive security protecting measure-Honeynet," *Computer Engineering*, vol. 28, no. 12, pp. 9-11 (in Chinese), 2002.
(刘宝旭, 许榕生, "主动型安全防护措施-陷阱网络的研究与设计", *计算机工程*, 2002, 28(12): 9-11。)

[68] Liu Baoxu and Yang Zeming, "The Study on the Technologies and Applications of Network Trap," *Information Security & Technology*, vol. 2010, no. 7, pp. 19-22 (in Chinese), 2010.
(刘宝旭, 杨泽明, "网络陷阱技术: 主动防御的基石", *信息安全与技术*, 2010(7): 19-22。)

[69] Jia Zhaopeng, Fang Binxing, Liu Chaoge, Liu Qixu, and LIN Jianbao, "Survey on cyber deception," J*ournal on Communications*, vol. 38, no. 12, pp. 135-150 (in Chinese), 2017.
(贾召鹏, 方滨兴, 刘潮歌, 刘奇旭, 林建宝, "网络欺骗技术综述", *通信学报*, 2017, 38(12): 135-150。)

[70] Juels A and Rivest R L, "Honeywords: Making password-cracking detectable", in Proc. the 2013 ACM SIGSAC *conference on Computer & Communications Security* (CCS'13), pp. 145-160, 2017.

[71] Farinholt B, Rezaeirad M, Pearce P, et al., "To Catch a Ratter: Monitoring the Behavior of Amateur DarkComet RAT Operators in the Wild," in Proc. 2017 *IEEE Symposium on Security and Privacy* (S&P), pp. 770-787, 2017.

[72] "Lions at the Watering Hole – The 'VOHO' Affair," The RSA Blog, http://blogs.rsa.com/will-gragido/lions-at-the-watering-hole-the-voho-affair/, Jul. 2012.

[73] "What is Spear Phishing? – Definition," Kaspersky Lab., https://usa.kaspersky.com/resource-center/definitions/spear-phishing.

[74] "Deceptions Everywhere," Illusive Networks, https://www. illusivenetworks.com/deceptions-everywhere/.

[75] "Unveiling 'Careto' - The Masked APT," Kaspersky Lab., https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf, Feb. 2014.

[76] "THE DUKES 7 years of Russian cyberespionage," F-Secure Labs, https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf, Sep. 2015.

[77] "Digital Bread Crumbs: Seven Clues To Identifying Who's Behind Advanced Cyber Attacks," FireEye, Inc., https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-digital-bread-crumbs.pdf, 2013.

[78] "白象的舞步——来自南亚次大陆的网络攻击", 安天安全研究与应急处理中心(Antiy CERT), http://www.antiy.com/ response/WhiteElephant/WhiteElephant.pdf, Jul. 2016。

[79] "Vault 7: Projects," WikiLeaks, https://wikileaks.org/vault7/#Scribbles, Apr. 2017.

[80] "DocuColor Tracking Dot Decoding Guide," Electronic Frontier Foundation, https://w2.eff.org/Privacy/printers/docucolor/

[81] Fang Binxing, Cui Xiang, and Wang wei, "Survey of Botnets," *Journal of Computer Research and Development*, vol. 48, no. 8, pp. 1315-1331 (in Chinese), 2011.
(方滨兴, 崔翔, 王威, "僵尸网络综述", *计算机研究与发展*, 2011, 48(8):1315-1331。)

[82] Fifield D., Lan C., Hynes R., Wegmann P., and Paxson V., "Blocking-resistant communication through domain fronting," in Proc. *Privacy Enhancing Technologies*, no. 2, pp. 46-64, 2015.

[83] "美人鱼行动(APT-C-07)长达 6 年的境外定向攻击活动揭露", SkyEye and HeliosTeam, http://zhuiri.360.cn/upload/APT-C-07.pdf, May. 2016。

[84] "潜伏的象群——来自南亚次大陆的网络攻击", 安天安全研究与应急处理中心(Antiy CERT), http://www.antiy.com/ response/The_Latest_Elephant_Group/The_Latest_Elephant_Group.pdf, Dec. 2017。

[85] "摩诃草组织(APT-C-09)来自东南亚的定向攻击威胁", SkyEye and HeliosTeam, http://zhuiri.360.cn/upload/APT-C-09.pdf, Aug. 2016。

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

[86] Le Blond S., Gilbert C., Upadhyay U., Gomez-Rodriguez M., and Choffnes D. R., "A Broad View of the Ecosystem of Socially Engineered Exploit Documents," in Proc. *the 2017 Network and Distributed System Security Symposium* (NDSS 2017), 2017.

[87] "5 in China Army Face U.S. Charges of Cyberattacks," The New York Times Company, https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html, May. 2014.

[88] "Indictment, Court One, Conspiracy to Commit Computer Fraud and Abuse", the United States District Court for the Western District of Pennsylvania, https://www.justice.gov/iso/opa/ resources/5122014519132358461949.pdf, May. 2014.

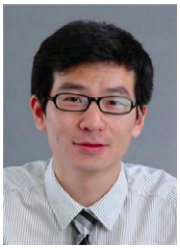
[89] "中方强力反击美方'起诉'中方人员", 中华人民共和国外交部, http://www.fmprc.gov.cn/web/wjdt_674879/fyrbt_674889/t1157508.shtml, May. 2015.

刘潮歌 于 2012 年在北京邮电大学计算机科学与技术专业获得硕士学位。现在中国科学院大学网络空间安全专业攻读博士学位。主要研究领域为网络攻击追踪溯源、Web 安全和网络欺骗。Email: liuchaoge@iie.ac.cn

方滨兴 于 1989 年在哈尔滨工业大学计算机系获得博士学位。现任中国电子信息产业集团首席科学家, 中国工程院院士。研究领域为大数据、计算机网络与信息安全。Email: fangbx@cae.cn

刘宝旭 于 2002 年在中国科学院研究生院核技术及应用专业获得博士学位。现任中国科学院信息工程研究所研究员、中国科学院大学网络空间安全学院教授。主要研究方向为网络与信息安全、攻防对抗、网络安全评测。Email: liubaoxu@iie.ac.cn

崔 翔 于 2012 年在中国科学院计算技术研究所信息安全专业获得博士学位。现任广州大学网络空间先进技术研究院研究员。研究领域为网络攻防技术。Email: cuixiang@iie.ac.cn



刘奇旭 于 2011 年在中国科学院研究生院信息安全专业获得博士学位。现任中国科学院信息工程研究所副研究员、中国科学院大学网络空间安全学院副教授。主要研究方向为网络攻防技术、网络安全评测。Email: liuqixu@iie.ac.cn

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net