互联网安全的40个智慧洞见

2015年中国互联网安全大会文集

360互联网安全中心 编

ISC 2015 中国互联网安全大会

360互联网安全中心

中国工信出版集团

人民邮电出版社 POSTS & TELECOM PRESS

互联网安全的40个智慧洞见

——2015年中国互联网安全大会文集

360互联网安全中心　编

人民邮电出版社
北　京

图书在版编目（CIP）数据

互联网安全的40个智慧洞见 ：2015年中国互联网安全大会文集 / 360互联网安全中心编. -- 北京 ：人民邮电出版社，2016.6
ISBN 978-7-115-42121-0

Ⅰ. ①互… Ⅱ. ①3… Ⅲ. ①互联网络－安全技术－文集 Ⅳ. ①TP393.408-53

中国版本图书馆CIP数据核字(2016)第080193号

内 容 提 要

本书站在互联网技术创新与应用实战的前沿，分别从网络空间与安全产业、大数据与威胁情报、政企安全与多维防御、新兴威胁与风险感知等四个角度为读者解析2015年中国及全球互联网安全的发展状态和演变形势，可供网络与信息安全相关科研机构以及高等院校研究人员、互联网安全领域企业技术与研发人员，以及对网络空间安全感兴趣的自学者参考。

◆ 编　　360互联网安全中心
责任编辑　李　静
责任印制　彭志环
◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路11号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京瑞禾彩色印刷有限公司印刷
◆ 开本：690×970　1/16
印张：28　　2016年6月第1版
字数：360千字　　2016年6月北京第1次印刷

定价：158.00元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315

序

从民用攻击的防御到高级攻击的捕获

齐向东

一、网络攻防的层次与演进

网络安全是一场无休止的攻防战，攻击技术、防御技术与安全服务都在这种不断的对抗中升级和演进。而与技术和产品同时进化的，还有我们对安全问题的关注点与认知。

十几年前，安全工作者们普遍关注的是木马、病毒、挂马、钓鱼等纯粹的民用安全问题。事实上，当网络终端缺乏基本有效的安全防护时，普通网民成为网络攻击的主要目标是必然的。当所有人都面临着同样严峻的安全威胁时，当每天都有几十万甚至上百万台电脑被木马感染时，很少会有人去关心那些隐藏在海量攻击事件中的个体差异。

进入21世纪的第二个十年，随着电脑安全软件以及第三方打补丁技术的普及，个人电脑安全保护问题得到了初步的解决，单个木马病毒的大规模传播事件已经基本绝迹。此时，移动互联网的安全性问题开始受到安全工作者们越来越多的关注。而特别值得一提的是，以CSDN泄密事件为标志，商业网站及商业系统的安全性问题，包括入侵、篡改、拖库、撞库、个人信息泄漏，以及DDoS（Distributed Denial of Service，分布式拒绝服务）攻击等，也都开始成为安全工作者们关注的重心和焦点。

而到了2015年，安全工作者们的关注点又再次发生了巨大的转变和飞跃。在这一年里，业界同仁们最爱谈论的前沿话题是“APT攻击”（Advanced Persistent Threat，高级持续性攻击），这是一种针对性、隐蔽性极强的网络攻击行为。而引发这场关注的是2015年5月，360发布的一份APT研究报告《OceanLotus数字海洋的狩猎者》。该报告披露了一个对境内特定目标持续攻击长达4年之久的境外专业黑客组织。这也是国内企业发布的首份专业的APT研究报告。报告发布后，立即引起了整个行业的关注和热议。随后，安天、绿盟、启明星辰等多家专业的安全厂商都纷纷展开了不同角度、不同程度的APT研究。

关于APT的研究，欧美国家起步较早，2006年就已经有相关的概念被提出，2010年以后开始受到广泛的关注。而国内关于APT的研究则相对起步较晚。造成这种情况的主要原因有以下几个方面。

第一，尽管国内安全厂商在民用安全技术方面已经处于世界领先水平，但APT攻击的针对性强，隐蔽性高，使用一般的、传统的民用安全技术，很难发现；

第二，APT 攻击的主要目标不是普通个人，而是特定的组织机构，包括政府、大企业和研究机构等，而国内传统的企业安全服务商，受到技术条件和相关体制的限制，大多不具备充分的数据收集和数据分析的能力，因此很难在实践中捕获真正的 APT 攻击；

第三，APT 组织大多拥有政府背景，相关研究比较敏感，国内安全企业在这方面的研究和成果披露都会比较谨慎。

不过，国内安全企业也有自己独特的优势。尤其是像 360 这样的互联网安全企业，其拥有的互联网技术与大数据技术的能力基础，是绝大多数国外安全厂商所不具备的。因此，虽然我们在 APT 方面的研究起步晚于欧美国家，但我们的进步却非常之快。截至 2015 年年底，360 威胁情报中心已经监测到针对中国境内目标发动 APT 攻击的境外高级攻击组织多达 29 个，其中 15 个 APT 组织曾经被国外安全厂商披露过，另外 14 个 APT 组织为 360 威胁情报中心首先发现并监测到的。而除了 360 之外，其他多家传统企业安全服务商也纷纷展开了各种与 APT 相关的安全研究，从而使 APT 的研究一下子成为行业研究的前沿热点。

APT 的研究与发现与传统的安全技术方法有很大的不同。传统的安全技术更加注重对已知威胁的防御能力。典型的检测方法就是用各种已知的样本对安全产品或防御系统进行测试，以查杀率和误杀率作为产品能力的评判指标。但实际上，随着网络形态的日益复杂化，未知威胁越来越多，特别是在 APT 等高级攻击中，未知威胁才是最主要的安全威胁。因此，能否发现或看见未知的威胁，就成为应对高级攻击能力的关键所在。

以 APT 为代表的高级网络攻击，无论是从攻击思想，攻击目标，攻击

技术，还是攻击影响来看，都与民用领域和一般商用领域的网络攻击有着巨大的不同。这也就使得我们不可能简单使用一般的民用安全技术来应对APT攻击。目前，国内外关于APT攻击的检测与防御技术有很多不同的方法。但从实践效果看，以大数据为基础的新型安全技术体系最具发展前景。

二、民用攻击与高级攻击的对比

一般来说，黑客针对普通网民发动的网络攻击是一种成本攻击和概率攻击，攻击目标并不确定，但攻击目的主要是为了获取经济利益。而如APT这样的高级攻击，则是一种价值攻击、定向攻击，攻击目标非常明确，攻击目的主要是情报窃取。如果做一个形象的比喻，一般的民用攻击就像是“入室行窃的小偷”，而高级网络攻击则更像是一个专业的“宝石大盗”。

入室行窃的小偷通常并不会选择固定的偷盗对象，也不是专门选定最有钱的住户去偷，而是会尽可能地选择那些容易得手的住户去下手。比如，一个小区里家家的窗户都装上了护栏，只有几家没有装，那么小偷自然就会优先从这几家没有安装护栏的住户下手。小偷之所以会这样做，实际上就是一种成本与收益的综合考虑，小偷也会综合考虑下手的难度、被抓的风险和盗窃收益之间的关系。有的人家很有钱，但如果下手难度太大，小偷就不会轻易下手。而且聪明的小偷一旦在一个住户那里得手，为了防止被抓，通常不会在同一个小区反复作案。

针对普通网民的网络攻击也是这样。攻击者总是会尽可能地选择那些系统没打补丁、没装安全软件、缺乏安全意识、防护水平较低的用户去下手。

至于被黑的人具体是谁，攻击者其实并不太关心。而攻击一旦成功，不论是盗号、劫持、钓鱼还是其他恶意行为，最终对用户造成的损失主要就是财产损失以及一定程度的电脑破坏。而且除非是用户在钱款被盗之后长期不采取任何有效的补救措施，否则，通常情况下，攻击者很少会在一个普通网民的电脑或手机上反复作案。骗成一笔，攻击者就会立即转向其他的目标。也就是说，电脑不装安全软件或安全软件不是最强的用户，是整个互联网安全的短板，这些短板用户是互联网上的重灾区。

而宝石大盗的做法则完全不同。宝石大盗一旦盯上了某颗宝石，不论其防护多么严密，都会想方设法去盗取；而且越是对于防护严密的宝石，越会采取长期的、有针对性的作案策划；以及相对比较复杂、高级的作案手段；在得到宝石之前不会轻易停手。这有点像我们熟悉的一部著名电影《碟中谍》中所讲述的故事：虽然主人公想要盗取的东西在一栋大楼里经过了层层严密的高科技保护，但主人公还是想尽各种办法，历经各种危险，最终成功盗取了被保护的东西。大有一种不达目的誓不罢休的劲头。

如 APT 这样的高级网络攻击也是如此。由于被攻击的组织的网络系统中存在着价值无法用金钱来估算的机密的情报信息，因此，攻击者会通过对目标机构、目标人群的长期研究和持续攻击，有的时候甚至是不计代价的网络攻击，来实现对机密信息的窃取。攻击者的攻击目标和攻击目的都非常的明确，他们既不会因为被攻击目标防御严密而罢手，也不会得手一次就跑路走人，而是会长期的、对同一目标进行持续不断的网络攻击，直至自己的攻击行为暴露为止。

高级攻击与民用攻击还存在其他一些明显的区别。

从攻击范围来看：在民用攻击中，攻击者往往会不断对大量不同的目标发动攻击，由于攻击的目标比较广泛，因此通常情况下都很难完全逃过安全软件的监控；但高级攻击则恰恰相反，被攻击的目标人群非常有限，甚至可能少到个位数，因此，被发现和监控的难度就非常大。

从攻击技术来看：在民用攻击中，攻击者所使用的技术手段通常不会特别高级，这一方面是由于开发者的水平有限——高水平的攻击者往往会选择价值更高的攻击目标而不是普通网民，另一方面也是由于攻击普通网民不需要太高超的技术水平，攻击者也会考虑攻击成本；但在有组织的高级网络攻击中，攻击者往往会使用非常复杂的技术手段，如免杀技术、加密技术、云控技术、环境分析技术、自我销毁技术，以及漏洞利用技术等多种高级技术手段，来尽可能隐藏自己并突破专业的安全防护。很多 APT 组织甚至能够利用多个高危 0day 漏洞发动攻击，使被攻击的目标防不胜防。

从攻击隐蔽性来看：在民用攻击中，尽管攻击者在攻击成功之前会尽可能地隐藏自己，可一旦目的达成，钱款到手，往往就会很快被受害者发现，并暴露自己的攻击意图，随后，攻击者就会立即跑路走人，正所谓“打一枪换一个地方”；但在高级网络攻击中，攻击者则始终会尽可能的长期隐藏自己，即使攻击得手，也还会继续隐藏自己并力求不断扩大战果。

从攻击途径来看：在民用攻击中，攻击者大多是通过社交工具、电商网站、电话短信、搜索引擎等公开途径对目标实施攻击，这些攻击大多处于公开或半公开的状态，很容易被第三方监测和发现；而在高级攻击中，攻击者最常用的攻击方式是鱼叉邮件和水坑攻击，前者是向指定攻击目标

发送含有恶意代码的邮件，后者则是在指定目标日常上网的必经之路上设置陷阱，这些攻击方法都比较隐蔽，不容易被第三方监测和发现。

例如，某 APT 组织黑掉了一个企业的官方网站后，在网站上植入了一个伪装成 Flash 更新的木马程序。当该企业员工访问这个网站时，就会看到 Flash 的更新提示，不明所以的员工一旦运行了更新包，电脑也就中招了。

从社会工程学角度来看：民用攻击中使用的社工手法大多具有通用性，至少是普遍适合某一类人群；而高级攻击中所使用的社工手法，针对性则特别强，攻击者甚至会长期对目标的业务领域、工作背景、行业情况进行长期深入研究后，再对目标展开社会工程学攻击。

比如，在我们已经截获的一些 APT 攻击中，攻击者向特定目标发送的鱼叉邮件中带有病毒，但邮件的标题和附件的文件名却很有针对性和欺骗性：如“国家 *** 的紧急通报”“最新 *** 照片与信息.jpg”“本周工作小结及下周工作计划”“2015 年 1 月 12 日下发的紧急通知”“商量好的合同”等。对于相关组织或企业的特定工作人员来说，一般很难识别出其中的破绽，他们很可能看到邮件后就会赶紧打开邮件并下载附件，于是电脑就中招了。甚至还有攻击者会冒充行业会议的组织者，与攻击目标进行很多轮次的邮件往来交互，最终才使目标成功中招。

三、民用攻击与高级攻击防御技术的对比

面对不同类型的攻击，安全策略也必然会有所不同。过去十年间，安全服务关注的大多是普遍发生的民用攻击，而在最近一两年间，高级

攻击的发现与防御才成为国内安全工作者关注的焦点。

从基本安全策略来看：对于民用攻击来说，安全服务考虑的重点自然是如何进行有效的防御；而对于高级网络攻击来说，则应以“一定防不住”为出发点制定安全策略，优先考虑的不是如何防，而是如何才能够看见和发现新的威胁。

从防护优先级来看：在民用攻击中，安全服务会优先查杀和防御那些攻击范围广、感染量大的木马病毒，而对于偶发的个例攻击，则可能会在兼顾效率的原则下，有选择地忽略；但在高级网络攻击中，即便是只有一个用户被攻击，安全服务也不能轻易的将其忽略，因为这一个用户就有可能是一个高价值 APT 目标。

从防御的深度来看：在民用攻击中，安全服务只要能成功阻止攻击，就算是防御成功了，通常不会特别关心攻击的源头和背后的攻击者；但在面对高级攻击时，安全服务就必须要具有关联分析和溯源分析的能力，因为只要攻击的源头还存在，那么对特定目标的攻击就不会停止。从这个角度看，民用攻击中的安全服务就像是小区保安，只管保护，不管抓人，也不管破案；而高级攻击中的安全服务则像是侦探或警察，必须有能力分析现场，追捕嫌疑人。

从核心技术手法来看：民用攻击的防御主要靠的是具体的攻防技术，包括驱动、引擎、沙箱、云端技术等多个方面；但高级攻击的发现主要靠的是数据技术，包括数据采集、数据分析与数据呈现等多个方面。没有大规模、翔实的数据记录，就不太可能发现那些隐蔽性极强的高级攻击；同样，如果没有足够效率的数据关联分析技术，也无法真正有效地

追踪攻击者的实时变化。当我们需要在一个企业的内部网络中发现高级攻击时，就需要对这个企业内部网络的数据进行充分的采集和记录；而当我们需要在整个互联网上分析或捕获高级攻击时，则需要我们对整个互联网的数据有充分的采集和记录，并且有足够的大数据处理能力来快速的从海量数据中捞出针一样细小的高级攻击事件。

四、新一代安全理念：数据驱动安全

数据驱动安全，这不仅是当下公认的新一代网络安全理念，同时也是2015年中国互联网安全大会的主题。数据能力必将成为未来安全企业竞争力的核心要素，特别是在高级网络攻击的发现过程中，数据的作用至关重要。那么，从安全的角度看，数据能力究竟包括哪些方面呢?

第一是安全数据的采集能力。

显然，数据本身是数据能力的基础，没有充分的数据采集，就谈不上任何的数据能力。而数据采集的能力又可以分为以下几个方面：一是安全数据的历史积累，如过去若干年的恶意样本库、恶意网址库、查杀记录等，这对于很多传统的安全企业和新入行的安全企业来说，的确是一个极大的挑战；二是最新安全数据的采集能力，这种能力主要取决于安全企业的终端用户数以及安全服务业务的覆盖面；三是相关领域的数据采集能力，因为安全事件并不是孤立的网络事件，它与网络服务器、DNS解析、网站页面内容等很多其他方面的网络信息密切相关，能够在多大的程度上采集相关领域的数据，决定了安全服务分析的范围以及有

多大的可扩展空间；四是数据采集的维度与粒度，只有足够丰富的维度和足够细密的粒度才能保证数据对真实攻击的呈现是充分的、完整的。

第二是数据的关联分析能力。

无论是在企业网络内部还是在整个互联网上，都会有各种各样不同的数据在不断地产生。但能否将这些数据进行有价值的关联分析，则是发现未知威胁和高级攻击的关键所在。比如，企业内网中可能部署了私有云、防火墙、IPS、IDS、终端管控、终端杀毒等多种安全产品，每个安全产品都会不断地产生各种安全数据，但由于这些产品往往来自不同的供应商，统计规则、统计角度也各有不同，所以它们之间的数据往往很难实现联动分析。

但实际上，数据之间往往存在着内在的关联性。例如，当防火墙监测到一个流量异常时，其对应的攻击可能是终端上感染了一个木马，如果终端与防火墙的数据能够进行真正有效的实时关联分析，我们就有可能形成联动效果和快速的威胁发现能力。所以说，能够将多少种不同维度、不同源头的安全数据进行有效的关联分析，也是数据能力的重要组成部分。

第三是机器学习的能力。

对于网络中实时产生的海量数据，完全使用人工分析显然是不可能的，这时，机器学习就显得特别重要。机器学习与人工智能技术，是大数据分析的必备能力。

以往，我们会使用机器学习技术来进行恶意程序的样本分析。360 自主研发的 QVM 引擎就是全球第一个通过机器学习技术实现的人工智能杀毒引擎，它很好地解决了海量样本的快速分析与识别问题。而现如今，

机器学习在很多其他的安全大数据领域也已经取得了突破。

比如，流量识别在传统安全技术领域一直是一个让人头疼的问题，特别是协议还原技术，既考验分析系统对层出不穷的各种网络协议的翻译能力，同时还会对服务器造成巨大的计算压力，成本很高。但现在，我们通过机器学习技术，已经可以实现在不解包数据流，不进行任何协议还原，甚至在完全不知道流量包采用的是什么通信协议的情况下，直接通过数据包本身特征分析，对流量进行快速的识别和分类，其准确性、识别效率和可扩展性都远远优于传统的方法。

第四是数据的快速检索与分析能力。

在网络对抗中，特别是与高级网络攻击的对抗中，分析的速度将决定对抗的胜负。如果攻击者可以在一分钟之内完成一次攻击，而分析者却需要用一个月的时间才能完成对这一次攻击的分析，那么即使等到分析结果出来了，也没有什么实际的意义了。所以，我们必须设法使数据分析与检索的速度能够与攻击者的速度相匹配，甚至比攻击者速度还要快。这时我们就会发现，如果能够将搜索引擎的大数据处理技术与互联网安全技术相结合，就会形成一个完美的组合。而这也正是现代安全大数据引擎技术的核心之一。

例如，在我们已经开发出来的天眼分析系统中，要从 90 多亿条恶意程序样本库中检索到某一个恶意样本的攻击历史及各种网络关联信息，检索时间仅为秒级。而这种超级的检索与分析速度，正是我们能够在仅仅不到一年的时间里，就捕获了 29 个境外 APT 组织，并且能够完整还原这些组织的攻击历史的秘密所在。

第五是数据的可视化分析能力。

不过，机器再厉害，安全问题也离不开人工专家的分析。但是，人的肉眼是很难直接读取海量的数据符号的，这就需要有可视化分析技术的帮助。可视化技术是现代网络安全技术的一项重要的辅助技术。安全数据的可视化技术可以帮助安全人员更加迅速而有效地分析安全问题，捕获安全线索，发现未知威胁。安全可视化技术是安全“看见”能力重要的“外在”表现形式。

比如，我们在世界互联网大会上展示的天眼系统，实际上就是一套前台展示可视化系统。该系统对各个高级攻击组织发动的历史攻击进行了一个可视化呈现。我们可以在系统中看到不同时间里，境外高级攻击组织对境内不同类型目标的攻击行为监测。这属于数据展示的可视化技术。

同时，可视化技术更重要的应用是数据分析的可视化技术，这是为安全分析人员使用的一种技术分析工具。比如，天眼系统的后台分析系统。运用这一系统，我们就可以快速地分析恶意样本、服务器以及受害者之间的关联，并迅速地定位网络攻击者。

五、未来的高级安全服务：威胁情报

如果我们在一个企业的内网系统中部署了足够多的数据采集设备，也完全有能力及时地分析和处理各种不同维度的安全数据，是否就已经具备了高级网络攻击的发现能力了呢？我们说，这还是远远不够的。因为一个单纯部署在内网系统中的数据监测与分析系统，还缺少一个最重

要的技术支撑——威胁情报。

这就好比我们去追捕一个金店劫匪，仅仅在金店里设置监控探头是远远不够的，我们还需要在店铺周边的街道上部署一系列的监控探头，这样才能够对劫匪的来路和去路进行全程追踪。发现高级攻击也是同样的道理。仅仅依靠企业自身网络的内部数据是远远不够的，还需要来自外部的，甚至是整个互联网上的数据情报，才有可能实现对高级攻击的完整分析。而这种来自外部的网络安全情报信息，就是威胁情报。

威胁情报的重要意义在于威胁信息的扩展与延伸。例如，我们在某个企业内部网络中截获了一个新的攻击样本，但单单凭借这一个样本，可能很难实现对攻击者的溯源和对攻击目的、攻击组织的深入分析。但借助安全服务商提供的互联网威胁情报信息，分析人员就有可能快速地找到更多的同源样本，发现若干的主控服务器，进而全景式地了解攻击者的攻击范围、攻击手法和攻击历史，甚至找到幕后的组织集团及其后台背景。当我们对攻击者的了解达到这种深度以后，即便不能完全消灭攻击者，也可以实现切实有效的针对性防御措施。

威胁情报的另外一个重要意义就是威胁的预警与提前防御。比如，某个大型企业遭到了 APT 攻击并且被我们截获，那么，跟它同类型的其他大型企业也很有可能遭到同一组织或同一手法的高级攻击。如果这个还未遭遇攻击的企业能够提前获得自身潜在攻击者的威胁情报，那么就完全有可能提前做好防御，避免攻击者的入侵。再比如，我们如果已经发现某类企业网站系统存在重大的安全漏洞，那么，通过威胁情报，就可以预警所有同类的网站尽快修复相关漏洞，以免被攻击。

我们在实践中还尝试了另外一种特殊的、全新的威胁情报获取方式，这就是安全舆情监测。我们通过搜索引擎技术，对全球所有的安全类网站、黑客社区和黑客社交账号进行了监测，通过关注“圈内人士”的关注热点，也可以提前获取很多潜在的攻击信息。例如，2014 年，我们就是通过这种方式从网上截获了一段“心脏出血”漏洞的攻击代码；而同年 Sony 被黑事件发生后，我们也发现，其实几个月前，就已经有知名的黑客组织在黑客社区里公开讨论如何攻击 Sony，并且被我们的安全舆情监测系统所截获。只是很遗憾，我们当时并没有充分意识到这一信息的重要性。但这些事例表明，通过安全舆情监测实现威胁态势的提前感知是完全可行的技术路线。

需要说明的是，威胁情报的产生方法并不唯一，但其中最重要，也是最具实际价值的产出方式，仍然是大数据的方法。

2015 年 8 月，360 成立了国内首个可以实际商用的威胁情报中心——360 威胁情报中心，目前已经有数十家国内外安全企业和互联网企业成为了 360 威胁情报中心的注册会员，并且 360 也已经开始以安全服务的形式，向我们的企业客户推送高价值的威胁情报信息。

六、结语

以 2015 年为标志，我们已经进入了数据驱动安全的新安全时代。而从民用攻击的防御到高级攻击的捕获，也意味着中国本土的安全企业在技术能力与服务水平上已经上升到了一个全新的高度，并且我们至少在某些方面，已经在全球范围内达到了领先的水平。