360追日团队APT报告：摩诃草组织（APT-C-09）

silence • 2016-08-06 09:38:09

一、概述：

摩诃草组织（APT-C-09），又称HangOver、VICEROY TIGER、The Dropping Elephant、Patchwork，是一个来自于南亚地区的境外APT组织，该组织已持续活跃了7年。摩诃草组织最早由Norman安全公司于2013年曝光，随后又有其他安全厂商持续追踪并披露该组织的最新活动，但该组织并未由于相关攻击行动曝光而停止对相关目标的攻击，相反从2015年开始更加活跃。

摩诃草组织主要针对中国、巴基斯坦等亚洲地区国家进行网络间谍活动，其中以窃取敏感信息为主。相关攻击活动最早可以追溯到2009年11月，至今还非常活跃。在针对中国地区的攻击中，该组织主要针对政府机构、科研教育领域进行攻击，其中以科研教育领域为主。

从2009年至今，该组织针对不同国家和领域至少发动了3波攻击行动和1次疑似攻击行动。整个攻击过程使用了大量系统漏洞，其中至少包括一次0day漏洞攻击；该组织所采用的恶意代码非常繁杂。载荷投递的方式相对传统，主要是以鱼叉邮件进行恶意代码的传播，另外部分行动会采用少量水坑方式进行攻击；值得关注的是，在最近一次攻击行动中，出现了基于即时通讯工具和社交网络的恶意代码投递方式，进一步还会使用钓鱼网站进行社会工程学攻击。在攻击目标的选择上，该组织主要针对Windows系统进行攻击，同时我们也发现了存在针对Mac OS X系统的攻击，从2015年开始，甚至出现了针对Android OS移动设备的攻击。

由于对摩诃草组织的攻击行动不是第一次披露，通过针对相应TTPs（Tactics, Techniques and Procedures，战术、技术与步骤）的分析，结合以往跟进或披露的各类APT组织或攻击行动，我们认为大部分APT组织的相关攻击活动是不会停歇的，即使被某些报告暂时披露，导致过去的手段失效，但是只要被攻击目标存在价值，攻击组织的行动依然持续；存在部分情况，攻击已达到最初预期，攻击组织选择暂时的蛰伏，但最终的目的也都是为了下一次攻

击养精蓄锐，这也是APT本身特性之一。其次，APT组织是否会对一个目标发动攻击，主要取决于被攻击目标的价值，而不在于被攻击目标本身的安全防护强弱程度，被攻击目标本身的强弱只是决定了攻击组织所需的成本，而大多数APT组织会为了达到其意图，几乎不计成本（具有国家背景的攻击组织所投入的攻击成本常常超出我们的想象）。

分析过去一年中发生的APT攻击，我们还发现中国一直都是APT攻击的主要受害国，其中相关攻击组织主要关注科研教育、政府机构领域，以窃取数据为目的。这和中国目前所处的经济与政治环境息息相关。同时，导致针对中国目标的攻击频频得手，除了被攻击目标本身防御措施薄弱以外，针对APT等高级威胁，被攻击目标本身缺乏积极主动的响应，即使在报告披露之后，甚至得知成为受害者之后，依然无法引起相应的重视，导致对自身检查和修复不足，常常旧伤未愈，又添新恨。

同时，中国网络安全行业依然缺乏能力型厂商的生存空间，大量的建设还是围绕过去的规划思路进行，这就导致了防护措施与高级威胁之间的脱节，从而给APT攻击造成了大量可乘之机。十三五规划的第一年，只有我们真正从安全规划上改变思路，积极引入能力型厂商，才能形成能力型安全厂商与客户之间的协同联动，打通监控发现到检测防御的事件响应各个环节，形成良性的闭合循环。

公开时间	报告名称	公司
2013 年 5 月 16 日	OPERATION HANGOVER-Unveiling an Indian Cyberattack Infrastructure[1]	Norman[2]
2013 年 5 月 20 日	Operation Hangover: Q&A on Attacks[3]	Symantec
2013 年 5 月 21 日	Big Hangover	F-Secure
2013 年 6 月 5 日	Operation Hangover: more links to the Oslo Freedom Forum incident[4]	ESET
2013 年 6 月 7 日	Rare Glimpse into a Real-Life Command-and-Control Server[5]	Crowdstrike
2013 年 11 月 5 日	Microsoft Office Zeroday used to attack Pakistani targets[6]	AlienVault
2013 年 11 月 5 日	CVE-2013-3906: a graphics vulnerability exploited through Word documents[7]	Microsoft
2013 年 11 月 6 日	Updates and Mitigation to Microsoft Office Zero-Day Threat (CVE-2013-3906)[8]	McAfee
2013 年 11 月 6 日	VICEROY TIGER Delivers New Zero-Day Exploit[9]	Crowdstrike
2013 年 11 月 7 日	THE DUAL USE EXPLOIT: CVE-2013-3906 USED IN BOTH TARGETED ATTACKS AND CRIMEWARE CAMPAIGNS[10]	FireEye
2014 年 6 月 10 日	Snake In The Grass: Python-based Malware Used For Targeted Attacks[11]	Blue Coat
2016 年 7 月 7 日	Unveiling Patchwork[12]	Cymmetria
2016 年 7 月 8 日	The Dropping Elephant – aggressive cyber-espionage in the Asian region[13]	Kaspersky
2016 年 7 月 10 日	白象的舞步——来自南亚次大陆的网络攻击[14]	安天
2016 年 7 月 25 日	Patchwork cyberespionage group expands targets from governments to wide range of industries	Symantec

表1安全厂商针对摩诃草组织发布的相关报告汇总列表

相关报道：

http://blogs.norman.com/2013/security-research/the-hangover-report

http://www.symantec.com/connect/blogs/operation-hangover-qa-attacks

http://www.welivesecurity.com/2013/06/05/operation-hangover-more-links-to-the-oslo-freedom-forum-incident

https://www.crowdstrike.com/blog/rare-glimpse-real-life-command-and-control-server/

https://www.alienvault.com/blogs/labs-research/microsoft-office-zeroday-used-to-attack-pakistani-targets

https://blogs.technet.microsoft.com/srd/2013/11/05/cve-2013-3906-a-graphics-vulnerability-exploited-through-word-documents/

https://blogs.mcafee.com/business/updates-and-mitigation-to-cve-2013-3906-zero-day-threat/

https://www.crowdstrike.com/blog/viceroy-tiger-delivers-new-zero-day-exploit/

https://www.fireeye.com/blog/threat-research/2013/11/the-dual-use-exploit-cve-2013-3906-used-in-both-targeted-attacks-and-crimeware-campaigns.html

https://www.bluecoat.com/security-blog/2014-06-10/snake-grass-python-based-malware-used-targeted-attacks

https://www.cymmetria.com/2016/07/12/unveiling-patchwork-apt/

https://securelist.com/blog/research/75328/the-dropping-elephant-actor/

http://www.antiy.com/response/WhiteElephant/WhiteElephant.html

http://www.symantec.com/connect/blogs/patchwork-cyberespionage-group-expands-targets-governments-wide-range-industries

二、摩诃草组织的四次攻击行动

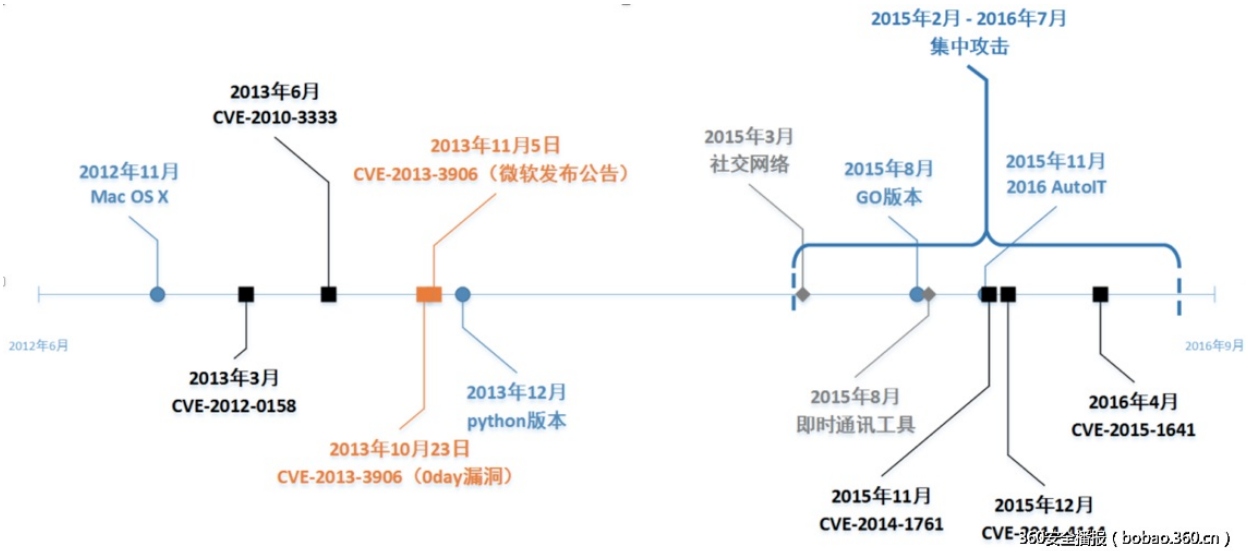

图1摩诃草组织相关重点事件时间轴

注：

1、圆形蓝色里程碑：相关典型后门首次出现时间

2、正方形里程碑：相关漏洞（CVE编号）首次出现时间

黑色：发起相关攻击时，漏洞为已知漏洞

橙色：发起相关攻击时，漏洞为0day漏洞

3、菱形深灰色里程碑：载荷投递首次出现的时间

攻击行动	活跃时间	载荷投递	漏洞利用	针对目标
第一次	2012、2013	鱼叉邮件（携带附件） 水坑攻击	CVE-2010-3333 CVE-2012-0158 CVE-2012-0422 CVE-2012-4792	主要针对巴基斯坦，涉及中国
第二次	2013	鱼叉邮件（携带附件）	CVE-2013-3906 （0day 漏洞）	主要针对巴基斯坦
第三次	2014、2015	鱼叉邮件（携带附件）	CVE-2010-3333 CVE-2012-0158	主要针对巴基斯坦，涉及中国
第四次 （疑似）	2015、2016	鱼叉邮件（携带附件） 鱼叉邮件（无附件） 即时通讯工具 社交网络	CVE-2014-6352 CVE-2015-1641 CVE-2014-1761 CVE-2012-0158 CVE-2014-4114	主要针对中国

图2四波攻击行动

第一次攻击行动：Norman安全公司于2013年曝光的Hangover组织，我们发现相关样本最早可以追溯到2009年11月，该组织在2012年尤为活跃，相关恶意代码和攻击目标的数量有不断增加。该攻击主要针对巴基斯坦，也有针对中国的攻击，但相关攻击事件较少。除了针对windows操作系统的攻击，在2012年针对Mac OS X操作系统的攻击也出现了。在第一次攻击行动中就已经开始利用漏洞进行攻击，但暂时没有发现该组织会利用0day漏洞。

第二次攻击行动：摩诃草组织在2013年10月下旬开始针对巴基斯坦的一次集中攻击，主要针对巴基斯坦情报机构或军事相关目标。本次攻击行动具有代表性的就是攻击中采用了一次利用0day漏洞（CVE-2013-3906）的攻击，该漏洞是针对微软Office产品，随后微软发布的漏洞预警指出该漏洞主要和TIFF图像解析有关。

第三次攻击行动：第二次小范围集中攻击之后，2013年12月底至2014年初，开始了新一轮攻击，相关目标主要还是针对巴基斯坦军事领域相关目标，本次攻击行动中除了C&C服务器等从网络行为可以联系上第一次攻击行动以外，从恶意代码本身代码同源性已经很难关联到第一次攻击行动了。这主要是本次攻击行动中的恶意代码大部分是用Python编写的脚本，然后使用PyInstaller 和 Py2Exe两种方式进行打包。

第四次（疑似）攻击行动：本次攻击行动也安全厂商被称为“Patchwork”或“The Dropping Elephant”，从2015年初开始持续至今的攻击，其中从2015年8月开始至2016年6月攻击非常频繁。本次行动的攻击目标主要是中国地区，期间使用了大量文档型漏洞，以CVE-2014-4114使用最多。我们主要通过本次攻击行动中C&C的SOA关联到第一次攻击行动中相关C&C历史域名注册人，由于SOA本身可以被DNS管理者修改，所以存在被刻意修改的可能性，但从我们的分析推断来看这种可能性很低，另外结合相关行动意图和幕后组织的发起方，我们更倾向本次攻击行动属于摩诃草组织的最新一次攻击行动。在本报告后续章节的研究分析，会将本次攻击行动作为摩诃草组织的第四次攻击行动进行描述。

三、中国受影响情况

本章主要基于摩诃草组织近期的第四次攻击行动，另外会涉及少量第三次攻击行动。进一步对相关攻击行动所针对目标涉及的地域和行业进行相关统计分析，时间范围选择2015年7月1日至2016年6月30日。

1.地域分布

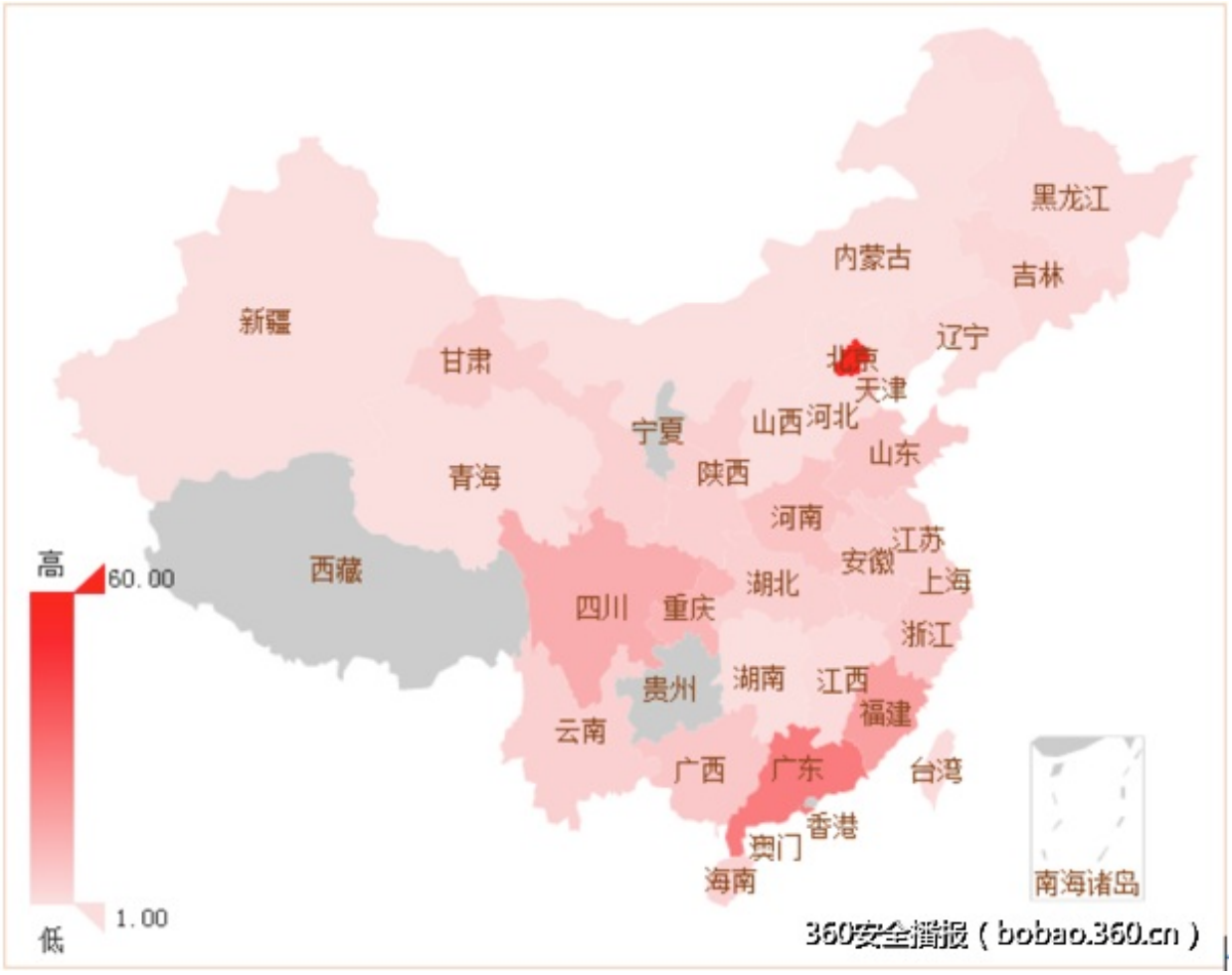

图3国内用户受影响情况（2015年7月-2016年6月）

国内受影响量排名前三的省市是：北京、广东、福建，其中北京地区是主要攻击目标，在西藏、宁夏和贵州这三个省市自治区暂未发现受影响的用户。

注：本报告中用户数量主要指追日团队监控到的计算机终端的数量

与第一次攻击行动类似，第四次攻击行动在针对中国的攻击中，科研教育领域依然是摩诃草组织重点针对的目标。

从第一次攻击行动开始军事领域一直是摩诃草组织关注的重点，期间主要是针对巴基斯坦地区，很少针对中国地区，但从2015年第三方和第四次攻击行动的开始，这一趋势逐渐改变，针对中国地区的军事领域的相关攻击不断增加。

四、载荷投递

关于针对中国的APT攻击中常使用的载荷投递方式，和主流的载荷投递方式的介绍，我们在《2015年中国高级持续性威胁（APT）研究报告》第四章中也详细介绍，读者可以结合参看相关报告。

1.鱼叉邮件

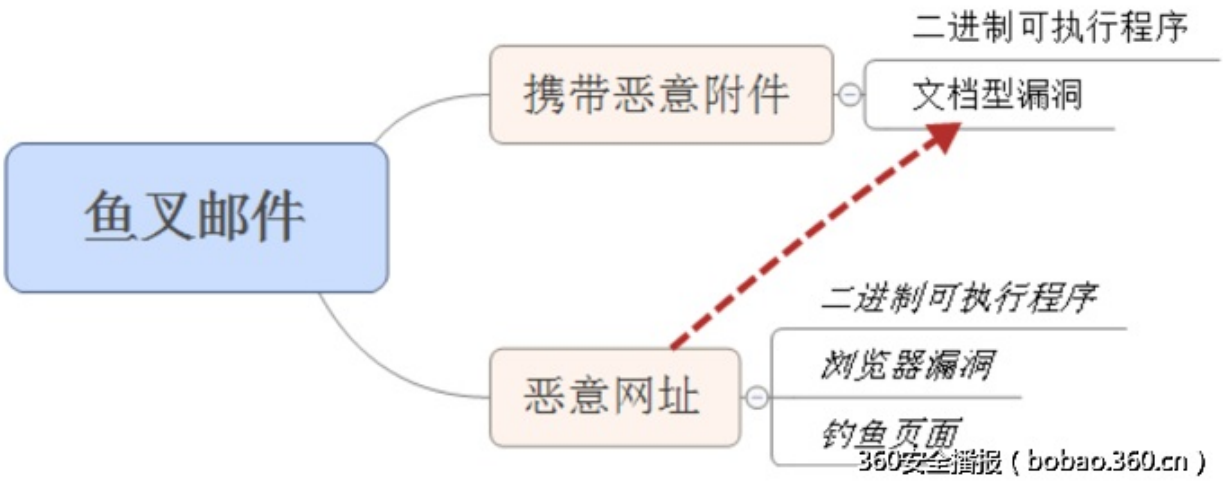

图5鱼叉邮件主要的类型

注：

上图中斜体字内容是摩诃草组织较少或从未使用的方式。

....

更多详情请下载完整报告:

PDF版本：https://yunpan.cn/c66LvX4xJx93G 访问密码 c4c2

相关推荐