RESEARCH
REPORT

2020

全球高级持续性威胁 APT

研究报告

- 2020年攻击概览
- 针对中国的APT攻击
- 全球威胁态势
- 2020年攻击态势总结
- 2020年攻击技战术总结
- 2021年APT趋势预测

360政企安全 360 高级威胁研究院

2020

全球高级持续性威胁

APT

研究报告

CONTENTS

05 070/2020年攻击技战术总结

06 079/2021年APT趋势预测

07 087/附录

摘要

基于360安全大脑全网安全数据和第三方公开情报数据综合研判，2020年高级持续性威胁整体态势如下:

- 2020年中国仍是APT攻击主要受害者，针对我国的攻击持续上升，其中政府、教育和国防军工相关单位是重点被攻击目标。我们今年共披露了23个APT组织涉及全球范围的攻击活动，针对中国地区发起攻击的组织13个。

- 全球范围内政府、国防军工依然是APT攻击的首要目标。今年发生了全球史上最严重的供应链攻击，致使全球31个国家数百家重要核心组织机构陷落。针对供应链的攻击，尤其是IT供应商的攻击未来将常态主流化。疫情背景下医疗行业的威胁凸显。伴随着5G和物联网技术的迅速发展，物联网设备已成为APT组织新的战备物资。涉及数字货币的攻击频发，这类新兴领域面临严峻挑战。

- 新冠疫情冲击下直接带来的是以聚焦远程办公突破口、围绕新冠疫情话题攻击、针对医疗行业窃取抗疫情报等使得APT威胁愈演愈烈。另一方面疫情全球化从多维度冲击着国际关系构建和国际秩序走向，安全秩序中的对立格局凸显，各方全面战略竞争加剧，由此刺激下的APT攻击威胁进一步加剧。

- 利用0day漏洞攻击持续活跃，但由于攻击成本高，供应链攻击的更高性价比，APT组织在选用0day攻击时会更加谨慎保守。越来越多的APT组织正在参与开发针对移动设备的武器工具。恶意通信流量与正常流量混合已成趋势，给现有流量安全检测带来巨大挑战。

- 意图为破坏、窃密的针对性勒索攻击将不断出现；越来越多的未知APT组织开始涌现，APT组织归属还需进行长期持续研判。另一方面更多的复杂攻击和全新组织将会陆续披露。

PART

全球高级
持续性威胁 APT
研究报告

01

2020年攻击概览

2020年初，在新冠疫情给全球格局带来新的冲击影响下，全球APT攻击活动异常活跃。全年公开报告数量687篇，其中涉及披露的组织132个，首次披露的组织25个。主要集中已知组织的新攻击活动，越来越多的未知APT组织开始涌现。另外我们也发现大量已知组织开始不断拓展战场，主要从攻击目标地域和涉及行业领域都有显著的变化，如海莲花组织更多采用攻击供应商策略，并更聚焦教育行业。“新冠肺炎疫情”已成为今年攻击利用最频繁的话题，在疫情影响下数字时代最大规模的一次远程办公迁徙，随之带来了一系列严重的安全问题，远程办公成为APT攻击“众矢之的”。全球范围内APT攻击活动涉及的领域主要围绕地缘政治涉及政府、国防军工、金融等，另外针对IT供应商、医疗行业的攻击显著上升，尤其是供应商问题越来愈严重，也是继APT组织使用0day武器后现阶段最优选的攻击战术。今年12月披露了针对SolarWinds公司供应链攻击的“落鹰行动”[1]，是全球史上最严重的供应链攻击，由此也暴露出供应商演变成全行业的安全短板。

境外APT组织针对我国的攻击持续上升，全年公开报告中涉及中国地区遭受攻击的报告数量最多，进一步依托360安全大脑和基于公开数据综合研判，我们发现2020年中国仍是APT攻击主要受害者。依托强大的安全能力，360在过去数年发现了44个其他国家背景的APT组织，监测到3000多次对中国的国家级网络攻击。我们今年共披露了23个APT组织涉及全球范围的攻击活动，针对中国地区发起攻击的组织13个，其中首次披露的组织4个，如魔鼠、蓝色魔眼和旺刺等组织。针对中国地区攻击的APT组织不仅数量最多，其攻击能力也是全球顶尖。

魔鼠（APT-C-42） **7月**

7月我们披露了该组织针对我国政府、通信等行业的攻击活动，并针对核心基础设施的供应商进行了渗透。相关攻击最早开始于2017年12月，持续活跃至今。

蓝色魔眼（APT-C-41） **10月**

我们监测到该组织在今年1月首次针对中国发起攻击，并捕获到了该组织最新V4版本的攻击组件。此次攻击的针对性极强，是该组织罕见地针对我国相关重要机构发起的首起定向攻击行动。

旺刺（APT-C-47） **12月**

12月我们披露了该组织利用ClickOnce恶意程序的攻击行动。这是一起来自朝鲜半岛地区未知APT组织的攻击行动，攻击行动可以追溯到2018年。

上半年，我们多次披露Darkhotel组织利用浏览器0day、VPN 0day等漏洞针对我国重要机构发起定向攻击。这些攻击组织使用大量0day、供应商战术、首次针对远程办公基础设施等最新技战术并不惜成本的首次应用在针对我国的战场上。

今年在新冠肺炎疫情和单边主义保护主义等多重压力之下，中国货物贸易进出口同比逆势增长1.9%，成为全球唯一外贸正增长主要经济体。由于地缘政治因素、新冠肺炎疫情的持续影响等长期问题，以及从针对我国活跃组织数量不断的增加趋势推测，尤其在围绕“十四五规划”和2035年远景目标等相关政策方向、新技术研究落地期间，这类多个APT组织都会窥探的领域，相关攻击会更活跃。我们预测明年针对中国的国家级网络攻击，活跃组织的数量和攻击活跃程度可能会超过今年。

360政企安全定位是“新时代的网络安全运营商”，向国家和所有城市输送网络安全运营能力，为国家、城市、行业构建安全防护“铜墙铁壁”。

PART

全球高级
持续性威胁 APT
研究报告

02

针对中国的APT攻击

360高级威胁研究院持续监控发现，针对中国地区的APT组织累计44个，监测到3000多次对中国的国家级网络攻击。2020年共披露了13个组织针对中国地区的攻击活动，其中首次披露的组织4个，如魔鼠、蓝色魔眼和旺刺等组织。今年境外APT组织针对我国相关重要机构或个人的攻击活动异常频繁，较去年持续上升，其中南亚、东南亚和东亚的APT组织最为活跃。相关攻击活动主要涉及我国政府、教育和国防军工相关单位，另外针对IT供应商和医疗行业的攻击大幅上升。

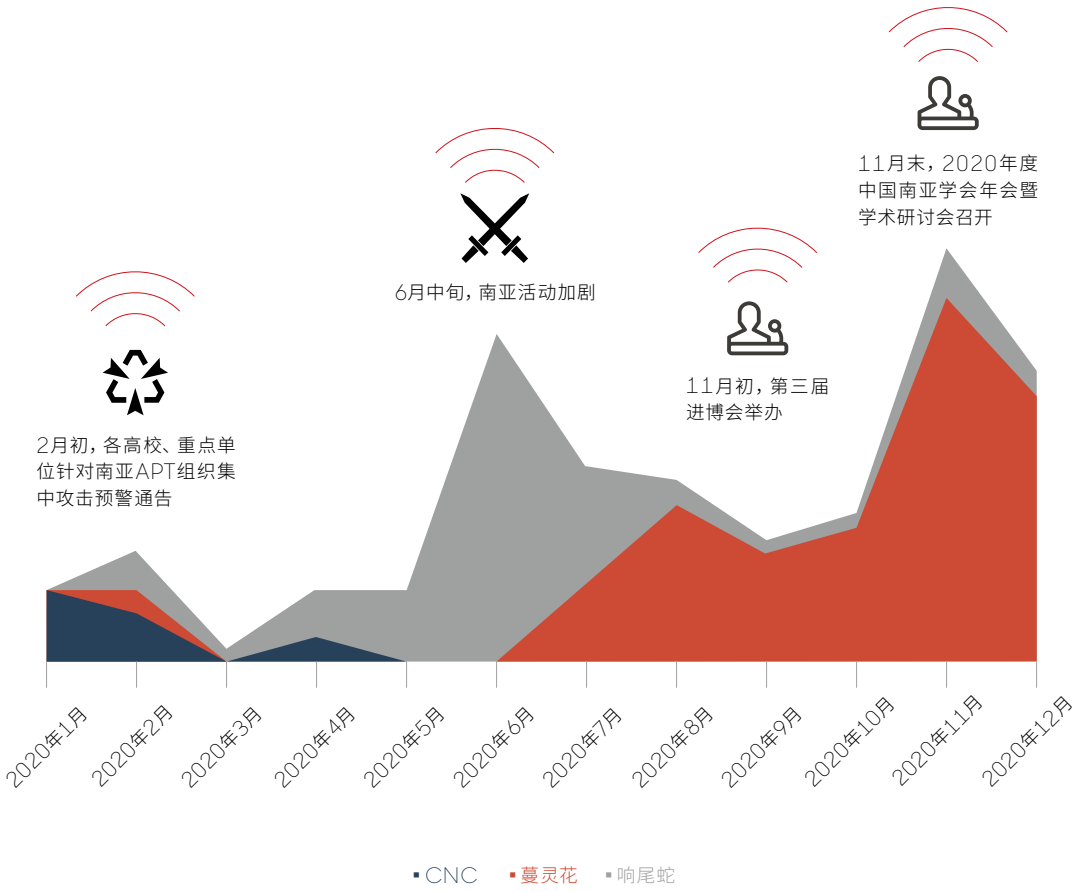
基于相关攻击频次、被攻击单位数量、受影响设备数量、技战术迭代频次等多个指标，我们对今年针对中国地区发起攻击的APT组织，相关攻击活跃度进行综合评估，其中老牌APT组织海莲花、Darkhotel和蔓灵花等组织长期持续活跃，而CNC、旺刺等组织更多是阶段性攻击活跃，TOP10组织列表具体如表所示。

排名	组织名称	涉及行业
TOP1	海莲花（APT-C-00）	政府、IT、教育等
TOP2	Darkhotel（APT-C-06）	政府、能源等
TOP3	蔓灵花（APT-C-08）	教育、国防军工、科研等
TOP4	毒云藤（APT-C-01）	政府、科研等
TOP5	响尾蛇（APT-C-24）	国防军工、政府、贸易等
TOP6	潜行者（APT-C-30）	通信、政府等
TOP7	魔鼠（APT-C-42）	IT、科研、通信等
TOP8	Lazarus（APT-C-26）	数字货币、政府等
TOP9	蓝色魔眼（APT-C-41）	军工、政府等
TOP10	CNC（APT-C-48）	国防军工、政府等

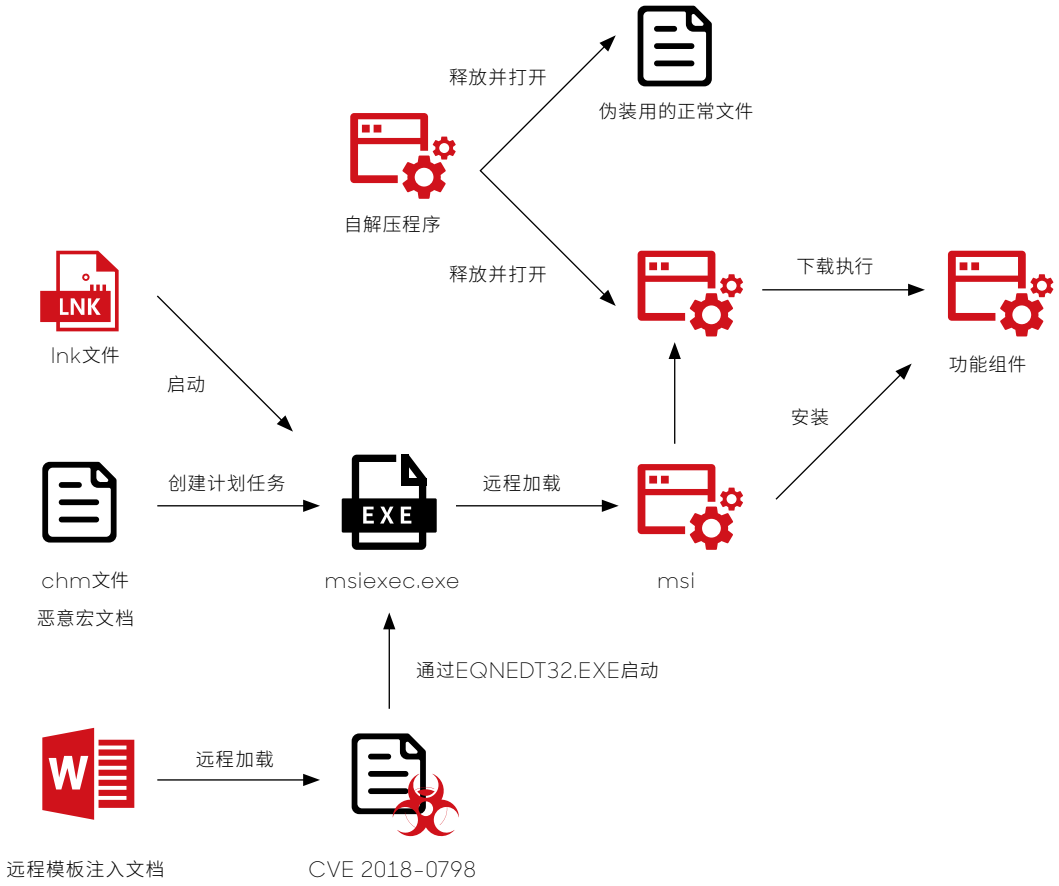
01 南亚

南亚地区主要活跃的组织是蔓灵花和响尾蛇，CNC组织主要在年初国内疫情爆发期间，针对重要单位发起集中攻击。2020年1月末，我们立即对相关重点客户进行预警加强防范，我们可以看到从2月中旬开始相关攻击已经收敛缓解。

但在短暂停歇后，从3月中旬开始响尾蛇、蔓灵花陆续展开集中大规模攻击，其攻击频次和目标范围较去年大幅增加。值得注意的是相关攻击会主要围绕热点事件展开，如6月响尾蛇针对某高校发起集中攻击；7月开始蔓灵花组织发起新的一轮攻击“季风行动”[2]；11月相关攻击活动非常频繁，尤其针对我国贸易和军工领域。



2020年南亚APT组织针对中国地区攻击趋势



1.蔓灵花 (APT-C-08)

蔓灵花组织，又被称 “Bitter”，”APT-C-08”，是一个针对中国、巴基斯坦等国家的 APT 组织。最早披露于2016年，主要针对军工、核能、政府等国家重点单位。蔓灵花组织在载荷投递的阶段手法较为多变，存在使用chm文件、恶意宏文档、远程模板注入文档、lnk文件和自解压程序等多种方式。但后续代码执行阶段则较为固定，通常为使用msi部署Downloader或直接释放Downloader下载其他功能组件。

蔓灵花主要攻击流程

其中，在今年9月份开始出现的chm文档中，蔓灵花会通过chm文件中内嵌的脚本创建计划任务周期性的从远程服务器加载msi文件。通过该方式达成无文件的Downloader。加大安全人员分析难度，提高其攻击流程结构的隐蔽性。

此外相关技战术与19年一致，通过克隆我国或巴基斯坦中敏感部门或机构的邮箱系统。通过投递邮件的方式，窃取用户邮箱账号和密码。对于今年发现的钓鱼邮箱网页，根据其模仿特点，可以分为四个批次。

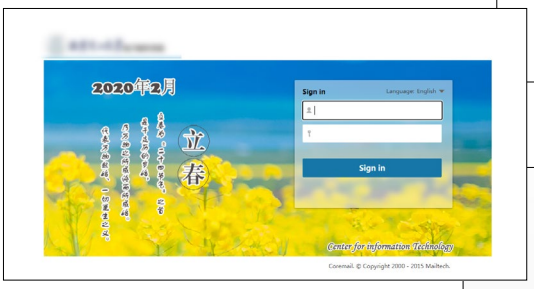


图 1

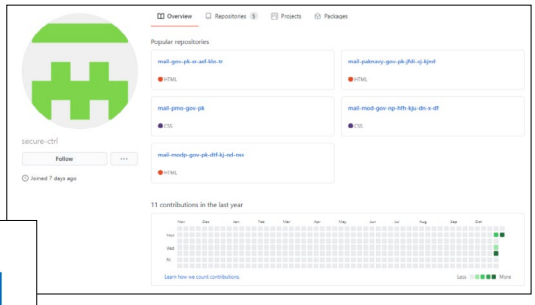


图 2

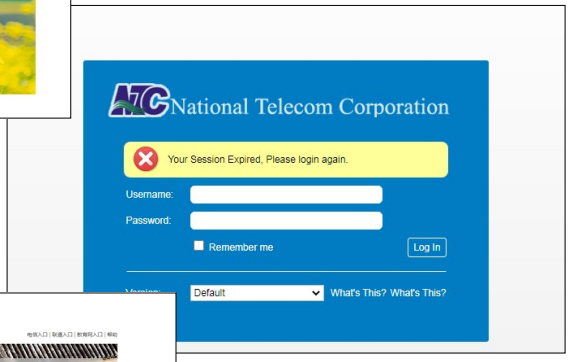


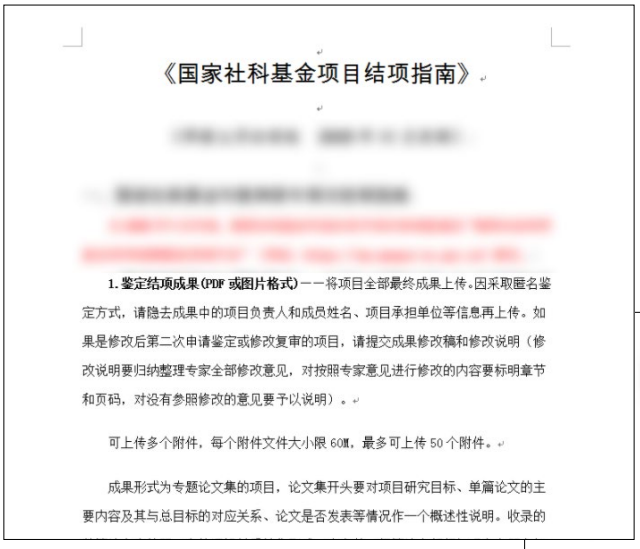
图 3

图 4

图1仿冒某大学邮件系统　图2 github部署钓鱼网站1　图3 github部署钓鱼网站2　图4 仿冒某大学邮件系统

此外，蔓灵花还在今年使用了多种技术成熟的公开远控，如QuasarRAT，AsyncRAT，DarktrackRAT以及价格高达$879.00/3个月的WarZoneRAT。

在攻击目标方面，相比往年，今年蔓灵花的攻击的频率在六月份以后大幅提高，主要针对贸易、军工和外交等方面。并且在11月份举办进博会的时间点前后，发起集中攻击，其中某外贸机构受影响严重。同时，还通过“国家社科基金项目.exe“以及”中国南亚语种学会2020年会邀请函.exe“等诱饵文档对我国研究南亚的社会科学学者进行攻击。



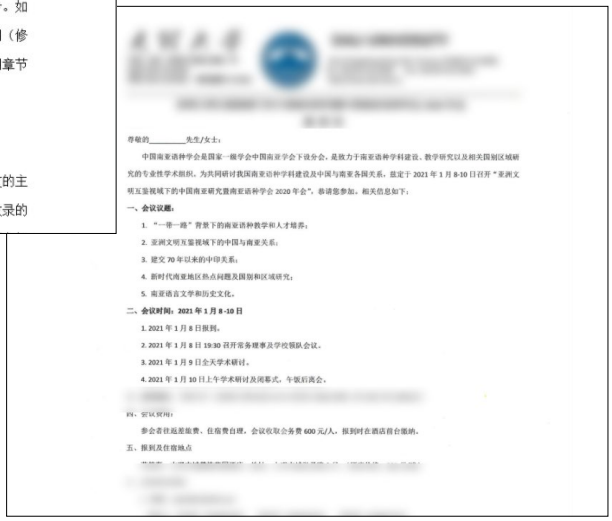
《国家社科基金项目结项指南》

1. 鉴定结项成果(PDF 或图片格式)——将项目全部最终成果上传。因采取匿名鉴定方式，请隐去成果中的项目负责人和成员姓名、项目承担单位等信息再上传。如果是修改后第二次申请鉴定或修改复审的项目，请提交成果修改稿和修改说明（修改说明要归纳整理专家全部修改意见，对按照专家意见进行修改的内容要标明章节和页码，对没有参照修改的意见要予以说明）。

可上传多个附件，每个附件文件大小限 60M，最多可上传 50 个附件。

成果形式为专题论文集的项目，论文集开头要对项目研究目标、单篇论文的主要内容及其与总目标的对应关系、论文是否发表等情况作一个概述性说明。收录的

图 5



尊敬的_____先生/女士：

中国南亚语种学会是国家一级学会中国南亚学会下设分会，是致力于南亚语种学科建设、教学研究以及相关国别区域研究的专业性学术组织。为共同研讨我国南亚语种学科建设及中国与南亚各国关系，拟定于 2021 年 1 月 8-10 日召开“亚洲文明互鉴视域下的中国南亚研究暨南亚语种学会 2020 年会”，恭请您参加。相关信息如下：

一、会议议题：

1. “一带一路”背景下的南亚语种教学和人才培养；
2. 亚洲文明互鉴视域下的中国与南亚关系；
3. 建交 70 年以来的中印关系；
4. 新时代南亚地区热点问题及国别和区域研究；
5. 南亚语言文学和历史文化。

二、会议时间：2021 年 1 月 8 -10 日

1. 2021 年 1 月 8 日报到。
2. 2021 年 1 月 8 日 19:30 召开常务理事及学校领队会议。
3. 2021 年 1 月 9 日全天学术研讨。
4. 2021 年 1 月 10 日上午学术研讨及闭幕式，午饭后离会。

四、会议费用：

参会者往返差旅费、住宿费自理，会议收取会务费 600 元/人，报到时在酒店前台缴纳。

五、报到及住宿地点

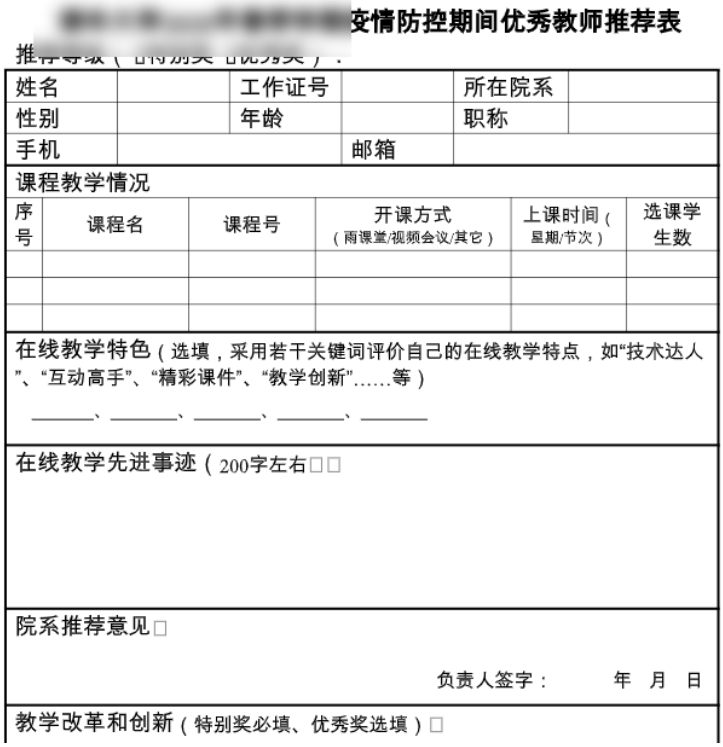
图 6

图5“国家社科基金项目”诱饵文档

图6“中国南亚语种学会2020年会邀请函”诱饵文档

2.响尾蛇 (APT-C-24)

响尾蛇组织在今年使用的攻击框架相对固定，主要使用lnk以及漏洞文档来进行攻击，通过JS反射来加载.Net程序，最终通过白样本利用驻留在受害者设备上。相关攻击活动主要针对我国军工、能源以及外交领域等。在今年6月中旬，响尾蛇使用“疫情优秀教师推荐表”相关文档针对某大学发起多起定向攻击，并在其中初次使用了“CVE-2017-0199”和“CVE-2020-0674”的组合漏洞文档进行攻击。



[redacted]疫情防控期间优秀教师推荐表

推荐等级（□特别奖 □优秀奖）：

姓名		工作证号		所在院系	
性别		年龄		职称	
手机			邮箱		

课程教学情况

序号	课程名	课程号	开课方式（雨课堂/视频会议/其它）	上课时间（星期/节次）	选课学生数

在线教学特色（选填，采用若干关键词评价自己的在线教学特点，如“技术达人”、“互动高手”、“精彩课件”、“教学创新”……等）

_____、_____、_____、_____、_____

在线教学先进事迹（200字左右□□

院系推荐意见□

负责人签字：　　年　月　日

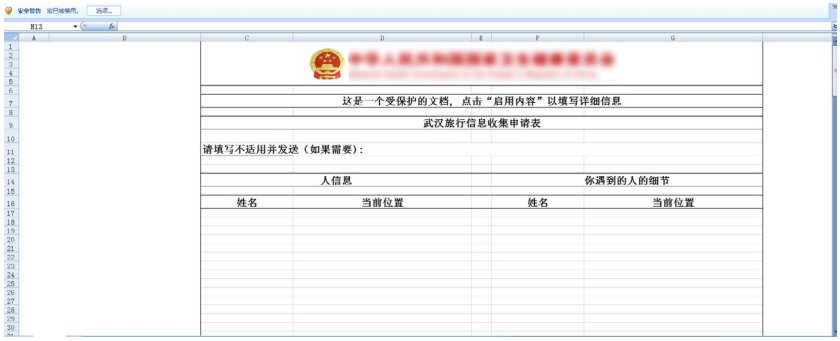
教学改革和创新（特别奖必填、优秀奖选填）□

响尾蛇投递的攻击样本种类繁多，但在使用的后门程序多为rekeywiz.exe的白利用，通过rekeywize.exe加载Duser.dll，进一步解密同一文件夹下的”.tmp”文件并加载至内存运行，通过创建两个定时器从服务器接收指令并执行对应功能，从而达到窃取设备上敏感信息的目的。此外，我们还捕获到响尾蛇使用C语言编写的Downloader，通过从服务器或注册表下载JavaScript脚本，反射加载.Net DLL。在其下发的JavaScript脚本中，我们捕获到三个不同功能的组件。

图“疫情优秀教师推荐表”诱饵文档

3.CNC (APT-C-48)

CNC组织是于2019年新出现的组织，由于其使用的远程控制木马的PDB包含了“cnc_client“的字样，所以将该组织命名为CNC。该组织主要攻击对象为我国军工和教育行业，并且在疫情爆发期间，通过伪造疫情相关的文档以及钓鱼网站对医疗行业发起攻击。



通过文档加载恶意宏或Shell.Explorer.1 OLE，从服务器下载专属远控程序到设备上。对设备进行远程控制。与其他南亚APT组织不同的是，该组织使用的CNC远控程序为64位环境编译，且CNC组织擅长使用其他多种语言。

有pyinstaller打包的py脚本，搜集目标设备上Chrome、360浏览器、UC浏览器和QQ浏览器的敏感信息，并上传到Dropbox上。也有go语言编写的远控程序，相关指令功能简单，具备了基本的持久化、键盘记录、窃取文件、屏幕截取等功能。

02 东亚

1.毒云藤（APT-C-01）和蓝宝菇（APT-C-12）

2020年初，在新冠疫情给全球格局带来新的冲击影响下，境外APT组织针对我国的攻击活动异常频繁。其中以毒云藤（APT-C-01）、蓝宝菇（APT-C-12）为首的东亚地区APT组织，相关攻击活动持续活跃。这两个组织均长期针对国内政府、军工、教育等领域的重要机构实施网络间谍攻击活动的东亚APT团伙，毒云藤其最早的攻击活动可以追溯到2007年，蓝宝菇可追溯到2011年。

2020年初，在国内抗击疫情期间，毒云藤组织利用新型冠状肺炎进行了钓鱼攻击，主要用于窃取目标用户邮箱账号和密码。后续使用各类诱饵主题的鱼叉邮件，针对特定目标投递lnk恶意附件安装后门程序等，6月初该组织开始针对特定单一目标开始实施钓鱼攻击。相比较来看蓝宝菇组织的攻击并不频繁，但持续活跃，而且今年8月在针对国内某重点机构的两次攻击活动中，该组织进一步升级了技战术。毒云藤11月有一次集中钓鱼攻击，这次目标依然主要围绕军工、高校相关企业单位。

东亚APT组织独有的战术特点是，相关攻击围绕军工行业周边相关单位进行迂回攻击，而较少直接针对具体军工单位发起正面攻击，但从2020年开始这一作战策略也开始尝试升级，即基于原有的迂回战术之外，也开始尝试直接攻击具体军工单位。

某博览会诱饵文档

2.Darkhotel (APT-C-06)

Darkhotel 组织是一个活跃十多年的APT组织，于2014年被卡巴斯基披露，攻击活动最早可追溯到2010年。该组织因针对入住高档酒店的商贸高管和国家政要而得名，攻击目标范围涉及中国、朝鲜、日本、缅甸等，主要目的是窃取敏感数据信息。该组织擅长使用漏洞攻击，尤其在0day漏洞储备方面非常丰富。

▪ 利用多个0day漏洞

年初，微软正式宣告Windows 7系统停止更新。在这个关键的时间节点，APT-C-06使用双星0day浏览器漏洞对中国商贸相关的政府机构发起攻击[3]，这两个0day漏洞分别是Internet Explorer浏览器漏洞 (CVE-2020-0674)，Firefox浏览器漏洞 (CVE-2019-17026)。此次攻击是利用office漏洞文档、网页挂马和WPAD本地提权的多种攻击方式进行的复杂组合攻击。这不是APT-C-06第一次使用浏览器0day漏洞，2018年360就披露过该组织利用“双杀”漏洞进行攻击活动，这些都表明该组织在漏洞方面深厚的技术储备。

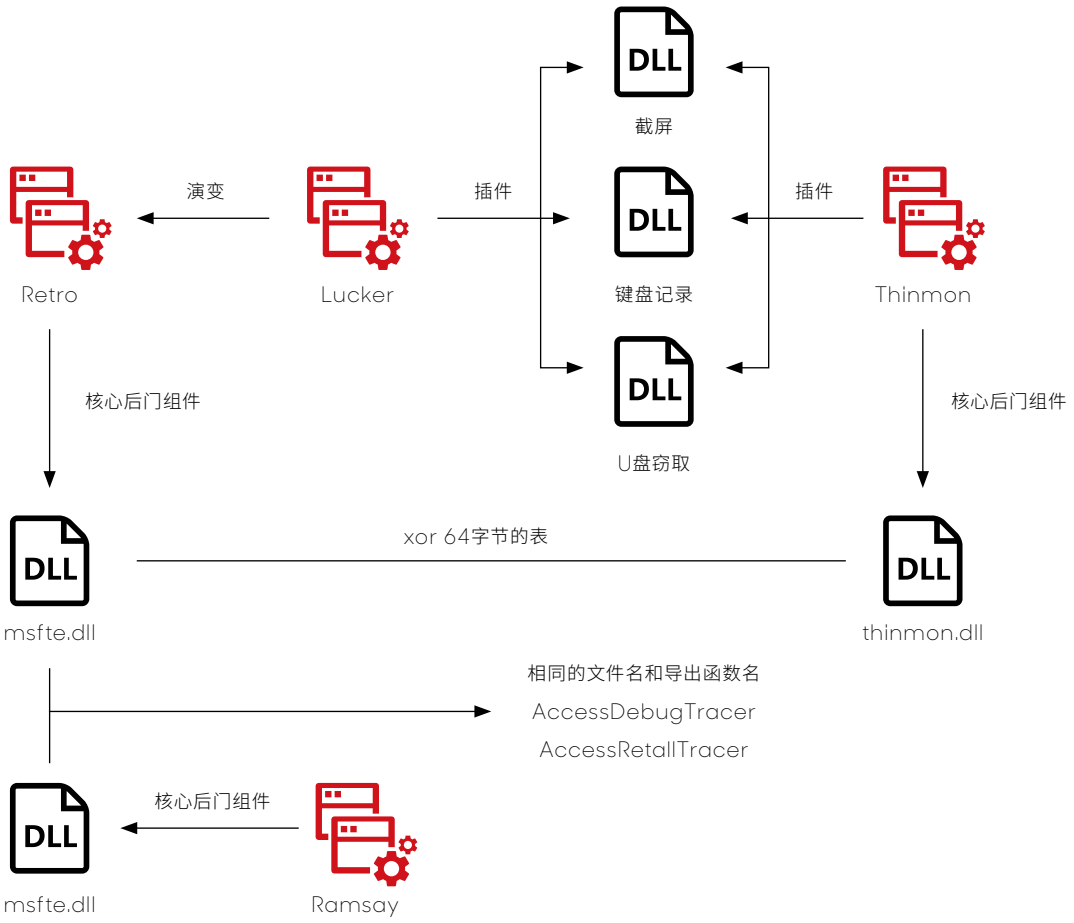
今年3月疫情期间，360安全大脑追踪发现DarkHotel组织通过利用国内某VPN软件0day漏洞，对我国驻外、政府等机构发起大规模攻击。期间DarkHotel使用了一个从未被披露过的全新后门框架——Thinmon。2020年公开报告中Darkhotel组织使用的0day漏洞均由360政企安全率先发现并预警防范。

漏洞编号	产品	补丁时间
SRC-2020-281	国内某厂商VPN	2020年4月7日
CVE-2020-0674	Internet Explorer	2020年2月11日
CVE-2019-17026	Firefox	2020年1月8日

2020年公开披露的DarkHotel组织0day漏洞利用情况

▪Thinmon和Ramsay家族

2019年6月，我们通过Darkhotel自定义的加密算法关联到新的攻击框架，该框架在插件部分于之前发现的lucker后门程序存在重叠，由于该框架的核心组件主要以thinmon.dll、wlbsctrl.dll以及其它一些文件名命名，因此我们将此次行动命名为thinmon，这次行动从2017年底一直活跃至今，今年3月（疫情期间）Darkhotel利用VPN供应链对国内实施大规模攻击，造成多个企事业单位近受影响。根据我们的研究发现，攻击者一般会通过内网环境的服务器（如，OA服务器、VPN服务器、安全软件服务端）下发并执行恶意脚本和含有thinmon组件的压缩包，恶意脚本会释放压缩包里的攻击组件并劫持相关服务，实现长期驻留。Thinmon框架主要用来加载其他插件模块。插件以加密的的形式存放在临时目录，只有在需要是才会被加载，插件功能包括屏幕截图、文件窃取、键盘记录、远程监控。



另外，今年五月份，ESET发布的研究报告《Ramsay: A cyber espionage toolkit tailored for air gapped networks》[4]，报告称他们发现了一个新型的网络间谍框架，并将其命名为Ramsay。该框架专为收集和泄露敏感文档而构建，并且可以感染包括移动介质内的其他正常文件，因此突破隔离网络是另一个主要特征。此外，报告里还提到Ramsay与Retro存在诸多关联，例如相同的Token、算法、文件名和技术等等。

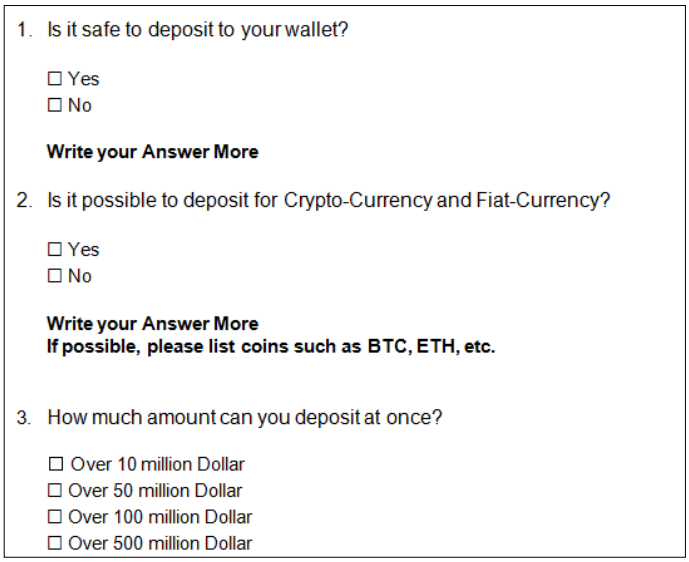
由于Thinmon和Ramsay都由Retro关联而来，因此我们认为他们可能为同一家族，可能因为应用场景和针对的目标不同，产生了不同的变种。但是他们又有很多的不同，Ramsay框架可以自身完成收集文件、与C2服务器通信等功能，并且还能感染其他文件，而Thinmon只能收集计算机基本信息、解密加载其他插件，没有通信、收集文件的功能，更不能感染其他文件。

3.Lazarus (APT-C-26)

APT-C-26(Lazarus 音译"拉撒路")是从2009年以来至今一直处于活跃的APT组织，据国外安全公司调查显示，该组织最早的攻击可能和2007年针对韩国政府网站大规模DDOS攻击的“Operation Flame”行动相关，同时可能是2014 年索尼影业遭黑客攻击事件，2016年孟加拉国银行数据泄露事件和2017年席卷全球的“Wannacry”勒索病毒等著名攻击事件的幕后组织。自2017年以来，Lazarus 组织将攻击目标不断扩大，日趋以经济利益为目的，从针对全球的传统金融机构银行系统进行攻击，开始转向于针对全球数字货币组织和相关机构以及个人进行攻击，尤其在近几年针对国内的攻击活动频繁活跃，多家数字货币交易平台已遭受攻击。

MATA框架是近期被卡巴斯基披露的一个多平台恶意软件框架，支持Windows、Linux和MacOS等多个主流平台，并拥有多个不同功能的攻击组件。该恶意框架的受害者广泛分布在波兰，德国，土耳其，韩国，日本和印度等地区，可能与Lazarus 组织存在关联。

今年9月，我们披露了《暴风行动 - Lazarus(APT-C-26)利用MATA框架针对数字货币行业的攻击活动揭秘》[5]。在MATA框架被披露后，360高级威胁研究院依靠360安全大脑针对MATA框架的攻击活动进行了追踪溯源，进而发现了一类利用MATA框架针对加密货币行业相关人员的攻击活动。众所周知，Lazarus组织近年来常以金融、数字货币等行业人员为攻击目标展开APT行动。从攻击目标的行业属性看，这次攻击活动所涉及的目标行业，也同样是Lazarus组织所感兴趣的。从攻击技术手法看，Lazarus组织近年针对数字货币行业的攻击，擅长改造相关行业所常使用的开源软件植入后门程序进行社会工程学攻击，而此次的攻击活动也使用了类似的手法。这些现象都间接显示MATA框架可能和Lazarus 组织存在关联。


1. Is it safe to deposit to your wallet?

☐ Yes
☐ No

Write your Answer More

2. Is it possible to deposit for Crypto-Currency and Fiat-Currency?

☐ Yes
☐ No

Write your Answer More
If possible, please list coins such as BTC, ETH, etc.

3. How much amount can you deposit at once?

☐ Over 10 million Dollar
☐ Over 50 million Dollar
☐ Over 100 million Dollar
☐ Over 500 million Dollar

图1

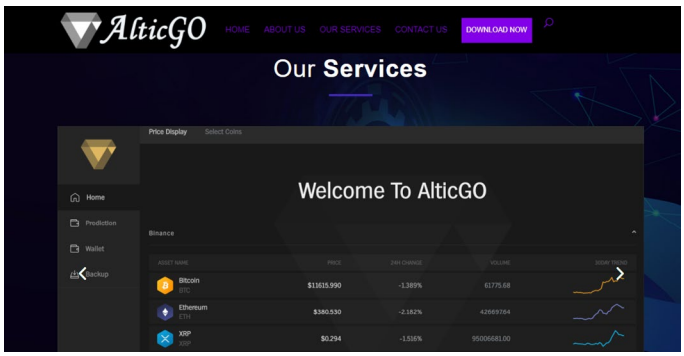
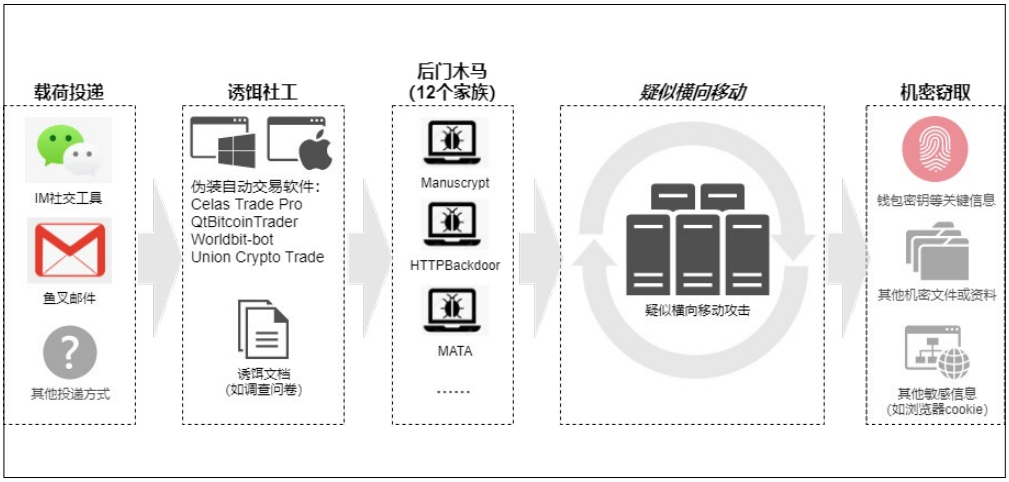


图2

图1 定制化调查文档　　图2 伪装成alticgo交易软件网站



步骤1: 利用鱼叉邮件或IM社交工具定向攻击数字货币从业人员;

步骤2: 进一步会投递伪装的交易软件或诱饵文档，伪装的交易软件有: alticgo、Celas Trade Pro、 Worldbit-bot、Union Crypto Trade、QtBitcoinTrader;

步骤3: 进一步捆绑的软件或诱饵文档最终会释放相关后门木马（12个家族），其中有代表性的主要是manuscrypt、HTTPBackdoor和MATA;

步骤4: 从Lazarus历史其他攻击活动技战术分析等，攻击者在获得单一目标权限后，并不能马上获得相关目标数据或密钥，还需进一步渗透拓展才能完全和持续掌控。但由于我们暂未发现具体的横向移动攻击行为，所以初步判定疑似相关攻击并且存在的可能性很高;

步骤5: Lazarus主要目标是窃取相应交易所热钱包私钥，由此达到窃取相应数字货币的目标，但从相关后门功能分析，完全具备窃取如浏览器敏感信息或文档数据等功能。以及Lazarus历史其他攻击活动分析，其攻击意图除经济犯罪以外，还会涉及很多政治目的。

通过对受影响用户初步分析，其中大部分是数字货币交易所人员，也有少量进行数字货币交易的普通用户。其中交易所主要涉及: OKEX、多比（Dobitrade）、中币(ZB)、富比特(FUBT)、D网数字（DAEX）等交易所。进一步基于鱼叉邮件、捆绑后门软件等分析，相关人员角色既有交易所管理层，也有具体开发运维等人员。

Lazarus组织窃取数字货币主要攻击流程

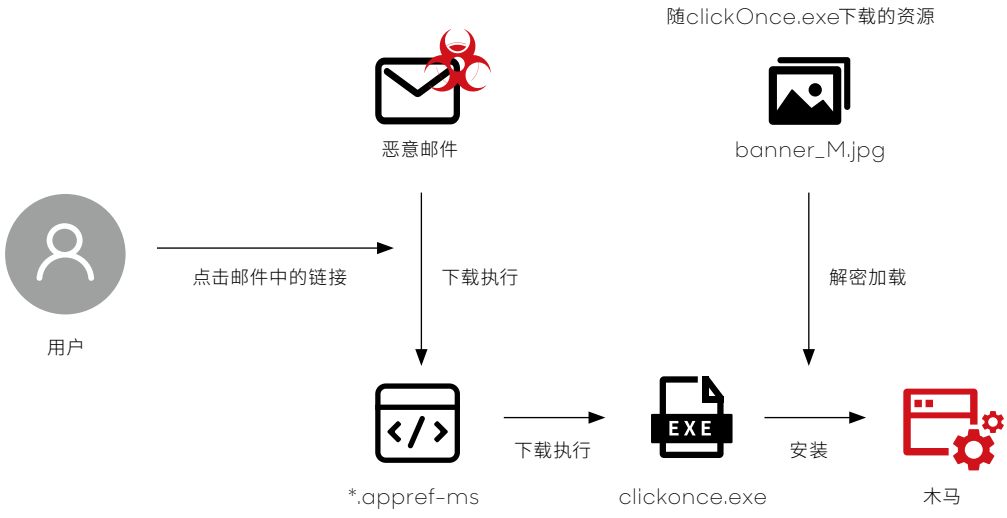
4.旺刺（APT-C-47）

360高级威胁研究院今年12月披露了“旺刺”[6]组织，该组织利用钓鱼邮件投递ClickOnce恶意程序的攻击行动。经过深入研判分析，发现这是一起来自朝鲜半岛地区未被披露APT组织的攻击行动，受害者涉及与半岛地区有关联的实体机构和个人，该组织的攻击行动可以追溯到2018年。由于此次攻击活动属于360全球首次捕获披露，我们根据该组织擅长攻击技术的谐音，将其命名为“旺刺”组织，并为其分配了新编号APT-C-47。

ClickOnce是近年来微软发布的一种软件部署技术，它可以创建基于Windows的自更新应用程序，让这些应用程序可以在用户交互最少的情况下安装和运行。2019年的美国Blackhat大会上，美国国土安全部所属CISA局的攻防专家曾公布了利用最新的ClickOnce扩展文件（.appref-ms）进行恶意攻击的技术原理[7]。该攻击方式区别于常规的恶意软件植入，由于微软设计的安装交互方式，使其非常容易被用于诱导安装恶意软件。

▪攻击流程分析

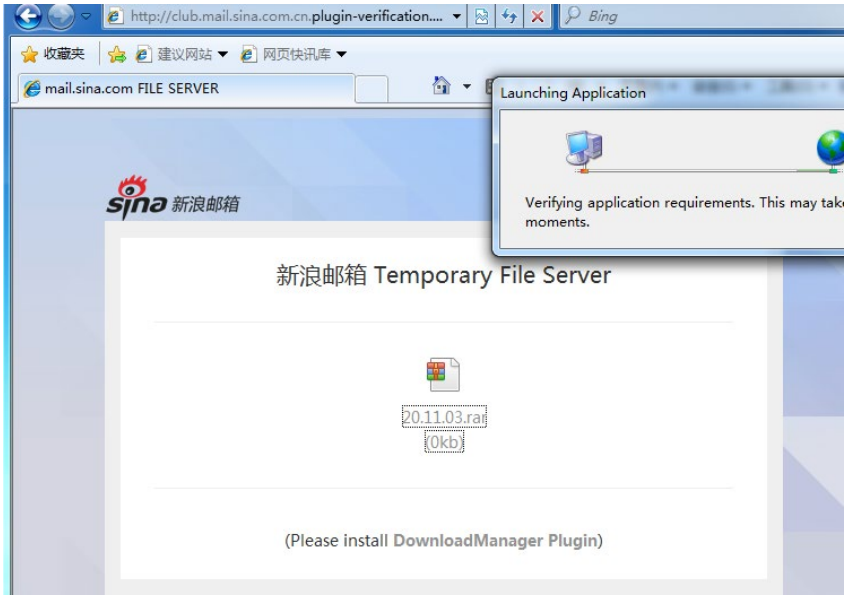
该组织通过向受害者投递包含伪装的安全插件升级钓鱼邮件实施攻击，当受害者点击伪装的升级钓鱼链接后会通过ClickOnce安装方式植入后门程序。完整的攻击流程如下图所示：



“点杀行动”主要攻击流程

▪ 钓鱼邮件分析

该组织伪装成某邮箱的安全团队向受害者发送邮件，诱导受害者升级邮箱安全插件。受害者进入伪装的插件网页点击安装链接，会下载安装ClickOnce程序的部署文件（*.appref-ms），appref-ms文件设置包含了恶意的ClickOnce程序地址。



恶意的ClickOnce程序安装完毕后，会欺骗用户安全模块更新完成。攻击者分别针对网易、新浪和outlook三类邮箱系统定制了伪装的安全模块部署网页。钓鱼域名和appref-ms文件对应，我们捕获发现最终下载的诱饵附件文件，是加密的word文档，名字和内容并不具有吸引力，所以攻击者钓鱼攻击的重点还是放在了伪装安全模块的诱导安装部分。

邮箱钓鱼页面

03 东南亚

1.海莲花 (APT-C-00)

海莲花 (OceanLotus) 组织，是一个有政府背景的境外黑客组织，攻击目标主要是东亚国家的企业和政府部门，从2011年中国就遭受到了海莲花组织的网络攻击，自2015年360曝光海莲花以来，该组织仍未停止过对我国的攻击。2020年海莲花是针对我国攻击中最活跃的组织，主要涉及到我国政府、IT和教育行业。今年该组织攻击技战术有明显提升，尤其基于供应链攻击成为今年主要的攻击手法之一，从3月开始针对我国多个大型IT供应商发起定向攻击，相关供应商的客户主要涉及国内教育、通信和政府行业等。

▪ 图片探针

今年2月海莲花在针对我国医疗机构的攻击活动中，初始攻击针对相关目标的大量邮箱发送了含有图片探针的探测邮件，用以探测攻击目标的邮箱是否真实存在。用户打开邮箱后在显示一张1X1像素不可见的图片后，会发送HTTP请求至海莲花的服务器，攻击者在服务端根据请求参数里的邮件地址，判断邮件是否被打开，以确定邮箱是否处于活跃使用状态。

图 1

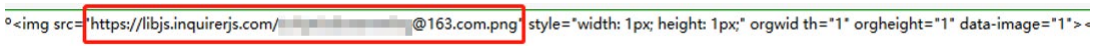


图 2

在探测确定邮箱活跃后，海莲花再通过白文件压缩包形式投递诱饵文档攻击用户，用户再打开压缩包点击白文件exe后，会加载同目录下的恶意文件。该攻击手法是海莲花组织惯用的白利用手法，白文件是某国产办公软件的主程序wps.exe，白文件wps.exe启动后会加载同目录下的krpt.dll文件执行。

图1 钓鱼探测邮件　　图2 图片探针

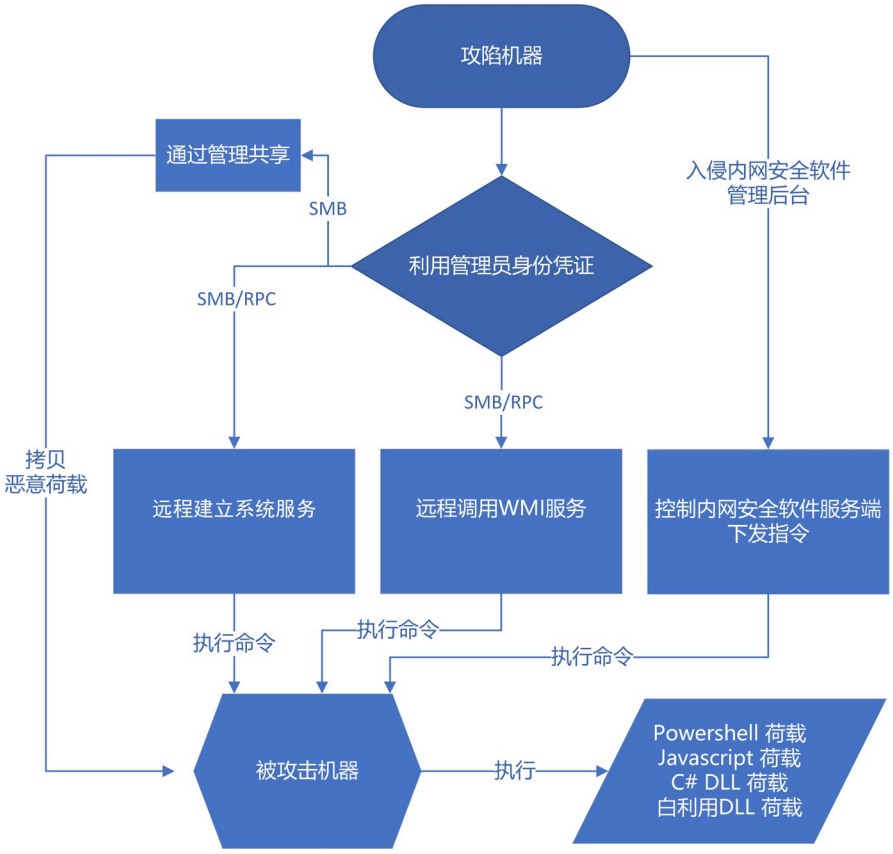
▪ 横向移动

海莲花在攻入企业内部后会进行较复杂的横向移动攻击，根据360安全大脑观测到的数据我们将海莲花的2020年核心的横向移动攻击技战术进行了梳理，主要攻击如下:

◇**远程建立服务**: 海莲花通过攻陷机器与被攻击机器windows管理共享建立连接,拷贝文件到受害者机器, 通过RPC调用远程建立服务来执行CMD命令;

◇**远程调用WMI服务**: 海莲花通过攻陷机器调用被攻击机器的WMI服务，通过WMI服务间接执行命令;

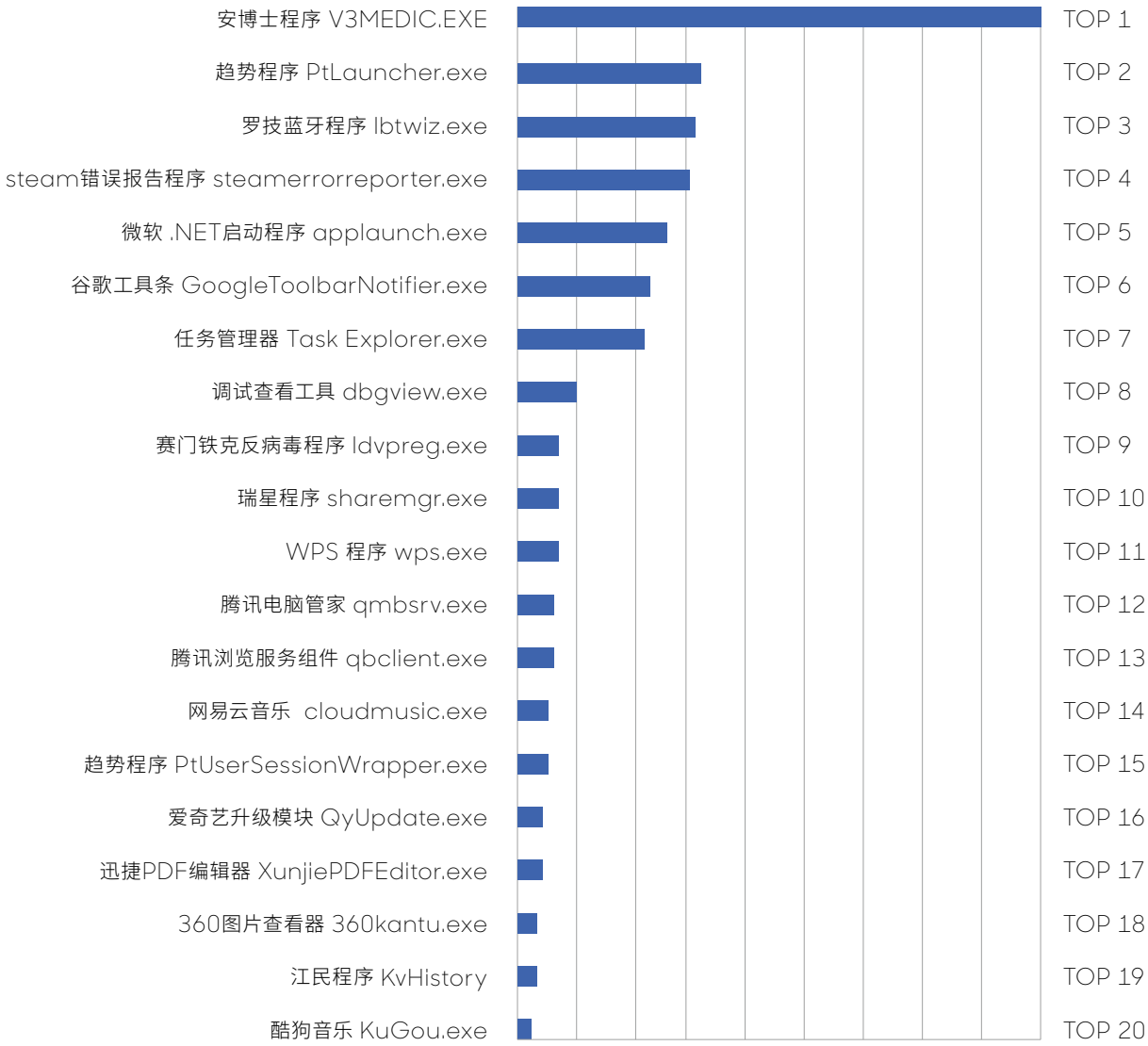
◇**控制内网安全软件服务端下发指令**: 海莲花在多次攻击活动中，疑似控制了内网安全软件的管理后台，通过对内网安装有安全软件的终端直接下发指令，执行命令安装后门程序。



海莲花横向移动攻击流程

▪白利用

DLL旁路加载技术是海莲花打造恶意荷载的核心攻击技术。下图被利用的白文件统计TOP20，利用最为频繁的是安博士程序。



海莲花白利用TOP20

04.其他

针对我国攻击活跃的APT组织，还有来自东欧地区的APT28（APT-C-20）、魔鼠（APT-C-42）。中东地区的蓝色魔眼（APT-C-41）组织。其中以魔鼠和蓝色魔眼相关攻击活动最为频繁。

1.APT28（APT-C-20）

2020年APT28组织针对我国的攻击活动中，以外交、政府相关重要机构为主要目标。利用多个语言，例如nim，delphi，go等版本的zebrocy downloader进行初始攻击，同时也在积极的利用不同的手法规避安全研究员的视线，在疑似针对北约组织目标的攻击活动中，依然使用压缩包附件形式的诱饵，但此次攻击使用了ARJ格式的小众压缩包格式，压缩包中包含一个nim zebrocy downloader和诱饵文档。压缩包的打包时间是2020年08月5号。同时在2020年的7月到8月我们捕获到了APT28的多个nim zebrocy downloader测试版本。

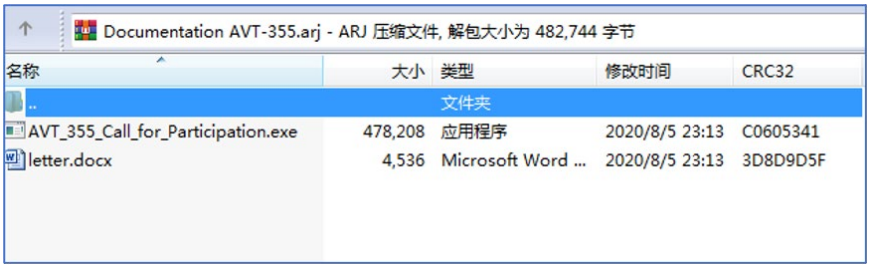


图1

图2

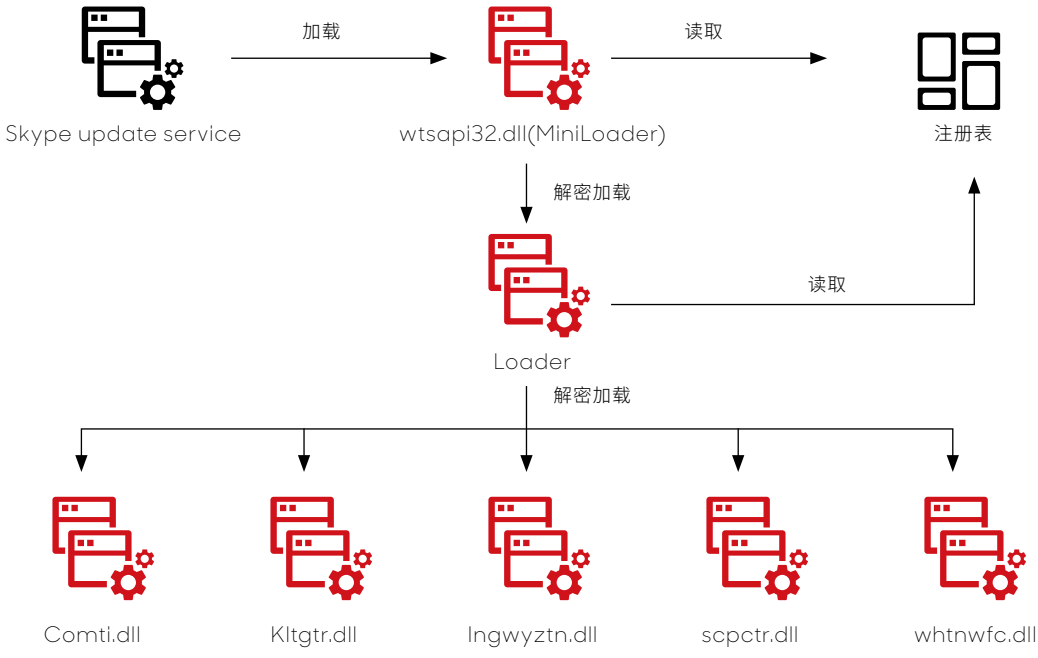
图1 APT28组织所使用的ARJ格式小众压缩包

图2 APT28组织诱饵文件涉及军事公告（新冠疫情下波兰边境军队活动的指示）

2.蓝色魔眼（APT-C-41）

蓝色魔眼（APT-C-41），又被称为Promethium、StrongPity，该APT组织最早的攻击活动可以追溯到2012年。该组织主要针对意大利、土耳其、欧洲等地区和国家进行攻击活动。360安全大脑监测到该组织在2020年1月首次针对中国进行了攻击活动，并捕获到了该组织最新V4版本的攻击组件。经过360高级威胁研究院的深入分析研判，此次攻击的针对性极强，是该组织罕见地针对我国相关重要机构发起的首起定向攻击行动[8]。

从历史攻击活动看，蓝色魔眼组织的攻击战备资源充足，具备0day漏洞作战能力，拥有一套复杂的模块化攻击武器库，并长期持续迭代更新。该组织的基础网络资源丰富，足以在每次攻击活动中有多套备用资源以便迅速更新持续对抗。早期该组织曾使用过0day漏洞发起攻击活动。而后被披露针对目标用户进行水坑攻击，伪装成用户常用合法软件或仿冒相关应用官方网站，从早期伪装WinRAR、TrueCrypt、Opera浏览器等软件，扩展到伪装TeamViewer、WhatsApp等应用软件。同时该组织还曾被发现一些ISP级别的网络劫持攻击活动迹象。该组织的攻击组件从2016年至今在不断进行升级改进，基于360安全大脑遥测数据来看，该组织的攻击组件至少已经有4次较大的更新迭代，今年活跃的主要是V3和V4两个版本。



蓝色魔眼攻击流程

3.魔鼠 (APT-C-42)

2019年，360高级威胁研究院捕获发现了一系列WellMess(APT-C-42)组织针对我国政府、通信IT行业、教育科研行业的APT攻击行动，并针对核心基础设施的供应链目标进行了渗透。因Golang语言的吉祥物为地鼠，与此同时“Mess”谐音 “Mice”，360安全大脑将这例新APT组织命名 为“魔鼠”。今年7月我们对该组织的攻击行动进行对外披露[9]。魔鼠组织的攻击活动最早开始于2017年12月，持续活跃至今。该组织不仅在中国进行攻击活动，还有日本等国家也成为其攻击目标[10]。我们捕获到的攻击活动具备以下特点：

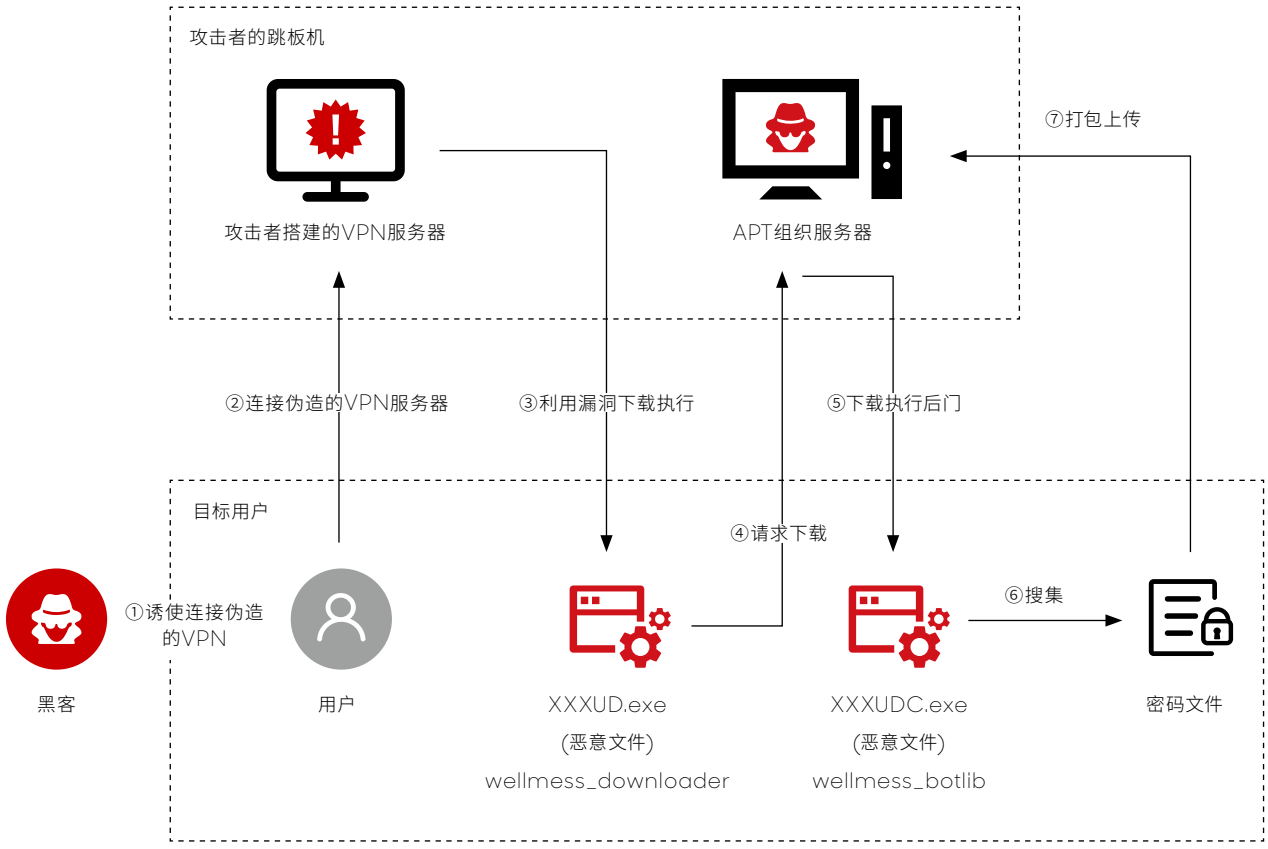
- **攻击对目标的针对性极强，对目标进行了较长时间的控制**
- **攻击进行了周密的筹划，针对目标发起了供应链攻击行动**
- **攻击所使用的后门程序具备windows和linux双平台攻击能力**

根据该组织攻击活动的轨迹，我们将其攻击活动划分为WellServ和WellVpn两次攻击行动。

- **WellServ行动主要是攻击目标的服务器，以长期持续控制和内网渗透为目的。**
- **WellVpn行动主要是针对网络基础服务供应商技术人员的定向攻击，以恶意VPN服务社工钓鱼作为切入点进行供应链攻击。**

WellVpn行动主要集中2019年8月-9月期间，以某网络基础服务提供商公司为目标，该公司的产品是各机构广泛使用的网络基础服务系统。进一步其核心攻击流程是利用VPN产品作为突破口。

某流行VPN产品的客户端升级程序存在安全漏洞，攻击者通过架设恶意的VPN服务器，通过社会工程学方式诱使该公司产品技术人员登陆，当技术人员使用存在漏洞的VPN 客户端连接恶意的VPN服务器时，将自动下载恶意的更新包并执行。攻击者下发的恶意程序是该组织的专属下载者程序WellMess_Downloader，下载并植入的最终的后门是WellMess_Botlib。整体攻击流程如下图所示：



魔鼠攻击流程图

PART

全球高级
持续性威胁 APT
研究报告

03

全球威胁态势

新冠疫情全球化影响下APT威胁加剧

2020年这场全球公共卫生危机，给全球带来生命和财产损害，也给全球化进程、社会治理、经济形态等人类诸多领域带来深刻影响。时至今日疫情的影响还在持续且未来1-2年内也很难结束，近期全球确诊人数已突破9000万。

新冠疫情冲击下，不少传统行业面临洗牌，但新的工作和生活方式也在疫情中涌现，远程

办公、线上学习、网上购物等，也凸显数字经济的重要性。但这方面直接带来的是以聚焦远程办公突破口、围绕新冠疫情话题攻击、窃取抗疫情报等使得APT威胁愈演愈烈。

另一方面疫情全球化从多维度冲击着国际关系构建和国际秩序走向，安全秩序中的对立格局凸显，各方全面战略竞争加剧，由此刺激下的APT攻击威胁进一步加剧，如南亚、东亚和中东等地区组织的攻击活动较去年显著上升，且不断浮现出更多未知归属的新攻击威胁。

全球史上最严重的供应链攻击

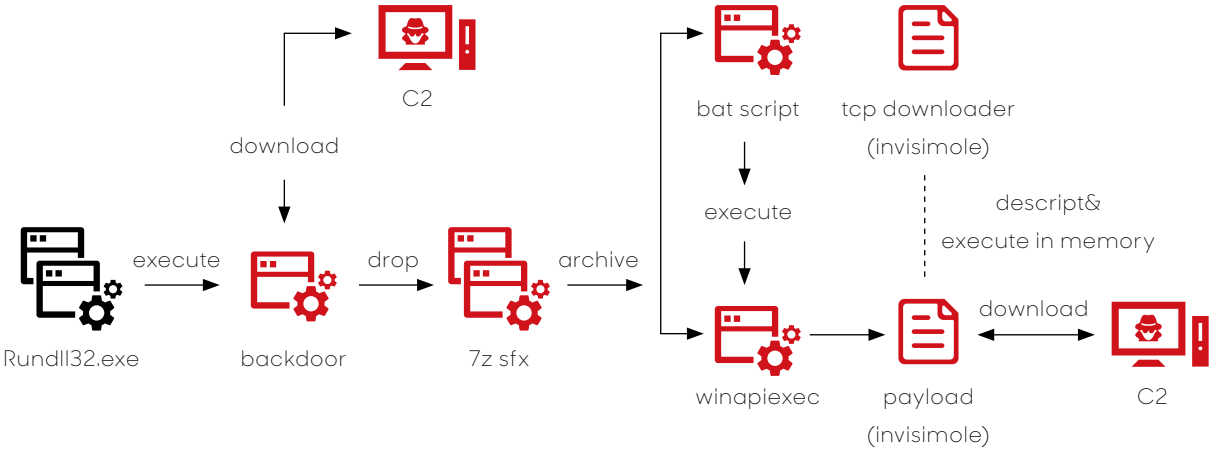
美国时间12月13日，SolarWinds公司Orion平台的多款软件被曝出植入了后门程序[11]，该公司为全球30万家客户提供了产品服务。360第一时间对此安全事件进行了预警，并独家发布了此事件的完整揭秘分析报告，该公司疑似在2019年就被黑客组织入侵，控制了该公司核心软件的编译发布流程，在该公司软件的官方安装包和在线升级程序包中的核心服务组件植入了后门程序。

根据360安全大脑的全网安全数据分析，我们发现了SolarWinds供应链攻击事件中数百家组织机构的失陷信息，这些组织机构共涉及31个国家，其中美国失陷的组织机构最多。此外，涉及18个行业，其中政府组织机构失陷情况最为严重，其次是金融和IT行业，同时有少量网络安全公司。可以说，这是一场史上最严重的供应链攻击，致使全球数百家重要核心组织机构陷落，给安全业界敲响了长鸣的警钟。

01 俄语系攻击组织

俄语系攻击组织众多，APT28、Gamredon、Turla、APT29等尤为活跃，相关组织主要针对欧洲、美洲等各国政府、军事机构。另外我们首次披露了某东欧组织针对乌克兰的最新定向攻击活动。

Gamaredon组织针对乌克兰的相关机构的网络攻击活动已经趋于常态化，并且该组织也在积极寻求横向移动和持久化技术。该组织也在积极的开发新的恶意软件对抗分析以及达到新的目的。在2020年我们捕获的针对乌克兰攻击活动中，我们发现了该组织配合invisiMole组织的攻击组件进行攻击，tcp downloader是InvisiMole组织研发的专属下载器，在2020年6月18号被ESET厂商首次披露[12]，而在此次Gamaredon部署的荷载正是InvisiMole组织的专属工具，这也是Gamaredon小组与InvisiMole小组联合行动的关键证据。这在以往的APT攻击活动中并不常见。



某东欧APT组织，2019年初，国外安全厂商披露了一起某东欧的APT组织针对乌克兰政府的定向攻击活动[13]，报告称该组织的攻击活动至少可以追溯到2014年。10月，360安全大脑监测到该组织针对乌克兰军事目标的最新攻击活动，该组织持续更新迭代网络武器，重点使用脚本类的无文件攻击方式，提高了安全厂商的发现和分析难度。同时该组织疑似通过云盘备份的方式窃取机密文件，此类攻击方式也加大了网络异常流量识别的难度。

该组织向目标投递了大量包含恶意CHM文件的ZIP压缩包，诱饵文件名称都使用了乌克兰语。在目标打开chm恶意文件后，恶意程序会通过powershell和vbs恶意脚本文件进行大量的文件窃取操作和植入木马行为。

Gamaredon与InvisiMole组织专属工具关联性

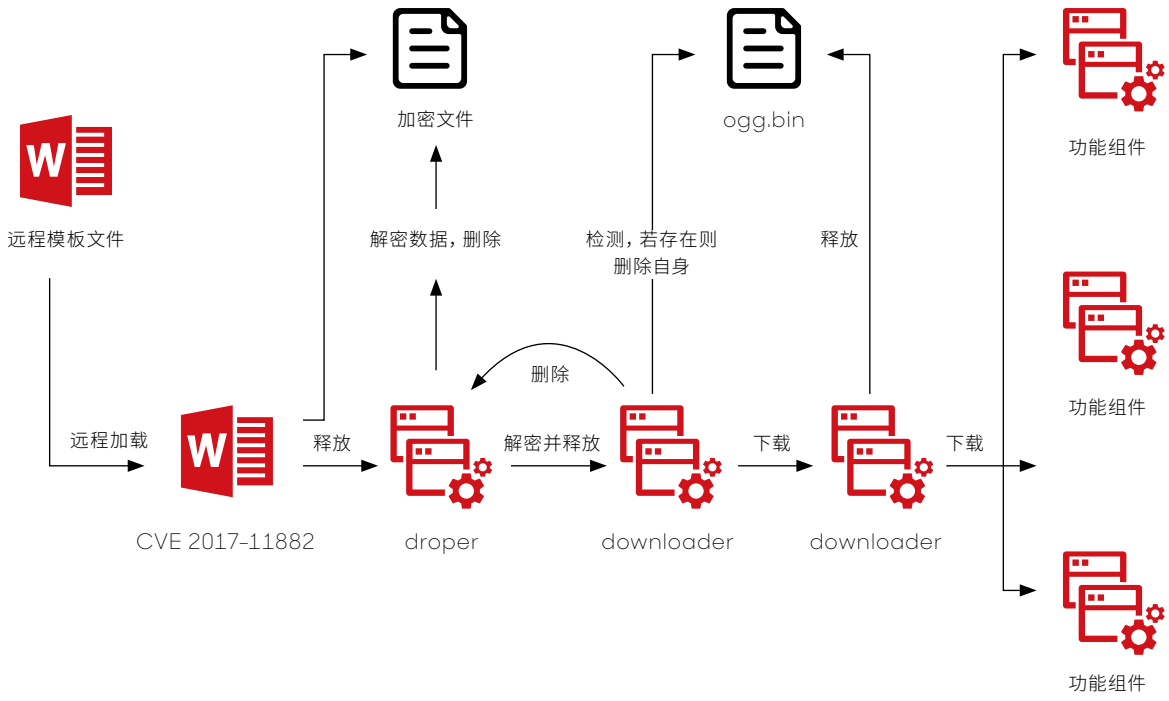
02 印欧语系攻击组织

印欧语系组织今年攻击非常活跃，除针对中国地区攻击以外，相关APT攻击活动主要集中在巴基斯坦、尼泊尔和印度等国家。印度与邻国巴基斯坦的关系急转直下，自1947年印巴分治，双方建国以来，双方对于克什米尔地区的主权纷争问题便未能得到解决。之后印巴之间发生过3次战争，而在克什米尔地区更是摩擦不断。在今年6月份双方分别驱逐对方外交官后，国际观察人士一致认为，印巴关系恶化程度甚至达到十多年来的最低点。

攻击活动	攻击时间
▪ **肚脑虫：** 持续对巴基斯坦政府、国防军工等机构进行攻击	1月 2月 3月 4月 5月 6月 7月 8月 9月 10月 11月 12月
▪ **蔓灵花：** 攻陷多个巴基斯坦网站，将其作为样本下发的载体	1月 2月 3月 4月 5月 6月 7月 8月 9月 10月 11月 12月
▪ **透明部落：** 持续对印度政府、国防军工等机构进行攻击	1月 2月 3月 4月 5月 6月 7月 8月 9月 10月 11月 12月
▪ **透明部落：** 伪装疫情、色情相关恶意应用攻击印度军事人员移动设备	1月 2月 3月 4月 5月 6月 7月 8月 9月 10月 11月 12月
▪ **摩诃草：** 攻陷巴基斯坦禁毒部队服务器"anf.gov.pk"，并进行水坑攻击	1月 2月 3月 4月 5月 6月 7月 8月 9月 10月 11月 12月
▪ **响尾蛇：** 使用疫情和海关预算等题材攻击巴基斯坦政府、医疗人员	1月 2月 3月 4月 5月 6月 7月 8月 9月 10月 11月 12月
▪ **蔓灵花：** 通过邮箱钓鱼网站对巴基斯坦国防军工、政府等部门进行攻击	1月 2月 3月 4月 5月 6月 7月 8月 9月 10月 11月 12月
▪ **摩诃草：** 使用国家网络安全、疫情等题材攻击巴基斯坦	1月 2月 3月 4月 5月 6月 7月 8月 9月 10月 11月 12月
▪ **响尾蛇：** 使用“一带一路”、印巴关系等诱饵文档攻击巴基斯坦	1月 2月 3月 4月 5月 6月 7月 8月 9月 10月 11月 12月
▪ **响尾蛇：** 使用“巴基斯坦-菲律宾协议”、NDS课程等题材攻击巴基斯坦	1月 2月 3月 4月 5月 6月 7月 8月 9月 10月 11月 12月
▪ **响尾蛇：** 针对移动平台的测试样本，涉及尼泊尔印度等内容	1月 2月 3月 4月 5月 6月 7月 8月 9月 10月 11月 12月

2020年印欧语系相关APT组织主要攻击活动

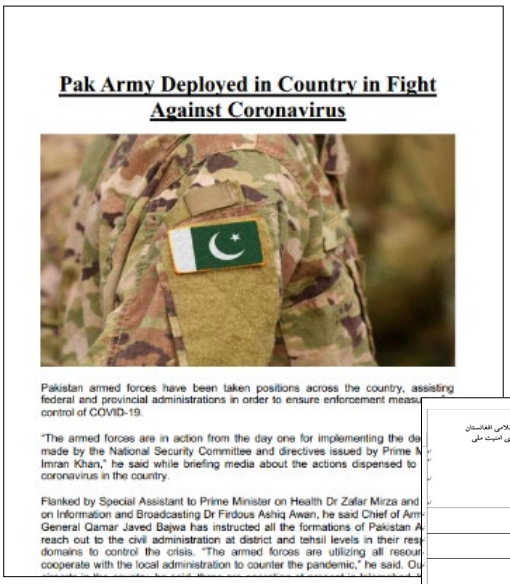
肚脑虫、蔓灵花、响尾蛇、透明部落几乎全年都有攻击活动，摩诃草更多在上半年持续攻击。印欧语系组织几乎都会涉及针对移动平台的定向攻击，肚脑虫、响尾蛇都涉及较多。今年年初趋势科技披露[14]，在Google Play商店中发现了响尾蛇组织使用的3个恶意应用程序，它们可以协同工作以破坏受害者的设备并收集用户信息。其中一个名为Camero的应用利用了CVE-2019-2215，该漏洞存在于Binder中，这是在野外首次利用所述UAF漏洞的实例。



肚脑虫组织（APT-C-35），又称Donot，是一个针对克什米尔地区相关国家的政府机构等领域进行网络间谍活动，以窃取敏感信息为主的攻击组织，相关攻击活动最早可追溯到2016年。今年该组织针对中国地区的攻击比较少见，主要持续活跃针对巴基斯坦相关政府、国防军工机构的攻击。

由于肚脑虫攻击流程较长，使用多个downloader，且在完成一个步骤之后会删除上一个步骤，极大提高其样本的隐蔽性，干扰安全分析员对其进行分析。相比其他印欧语系组织，该组织的后门程序在设备上驻留时间最长。

肚脑虫主要攻击流程



Pak Army Deployed in Country in Fight Against Coronavirus

Pakistan armed forces have been taken positions across the country, assisting federal and provincial administrations in order to ensure enforcement measu control of COVID-19.

"The armed forces are in action from the day one for implementing the de made by the National Security Committee and directives issued by Prime M Imran Khan," he said while briefing media about the actions dispensed to coronavirus in the country.

Flanked by Special Assistant to Prime Minister on Health Dr Zafar Mirza and on Information and Broadcasting Dr Firdous Ashiq Awan, he said Chief of Arm General Qamar Javed Bajwa has instructed all the formations of Pakistan A reach out to the civil administration at district and tehsil levels in their res domains to control the crisis. "The armed forces are utilizing all resour cooperate with the local administration to counter the pandemic," he said. Ou

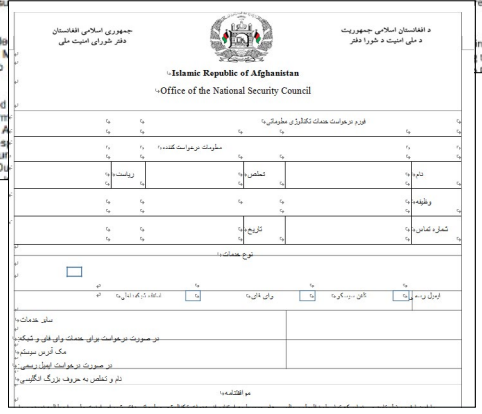
图1

Why Saudi ends loan and oil supply to Pakistan.

Saudi Arabia has ended a loan and oil supply to Pakistan due to the South Asian nation's criticism that the Saudi-led Organisation of Islamic Cooperation (OIC) is not doing enough to pressure India on the Kashmir issue, marking a new milestone in the deteriorating relations between the two allies. Pakistan was last week forced to repay a Saudi loan of $1 billion that the kingdom called in after

n November 2018, which to $3.2 billion. Those deals were Pakistan in February last year.

图2



Islamic Republic of Afghanistan

Office of the National Security Council

图3

透明部落组织是南亚APT组织，主要针对印度的军事与外交活动，在2020年广泛活跃，并且其攻击目标开始扩散到阿富汗等其他地区。透明部落组织今年年初使用开源的AhMyth RAT变体，用于在移动设备上进行监视。该变体主要在印度传播，伪装成与色情相关的应用程序和COVID-19跟踪应用程序用于入侵印度军事人员的手机。该组织主要使用Crimson RAT，今年8月卡巴斯基披露了该组织针对全球多个国家政府和军队的最新攻击活动[15]，其中Crimson中升级了新的USB蠕虫攻击组件，该组件可从移动存储设备中窃取文件并通过感染相关设备进行传播。相关攻击涉及27个国家，其中受影响最大的是阿富汗、德国、印度、伊朗和巴基斯坦等国家。

图1 响尾蛇使用疫情相关题材的样本攻击巴基斯坦

图2 摩诃草使用的漏洞文档 (CVE-2017-0261)

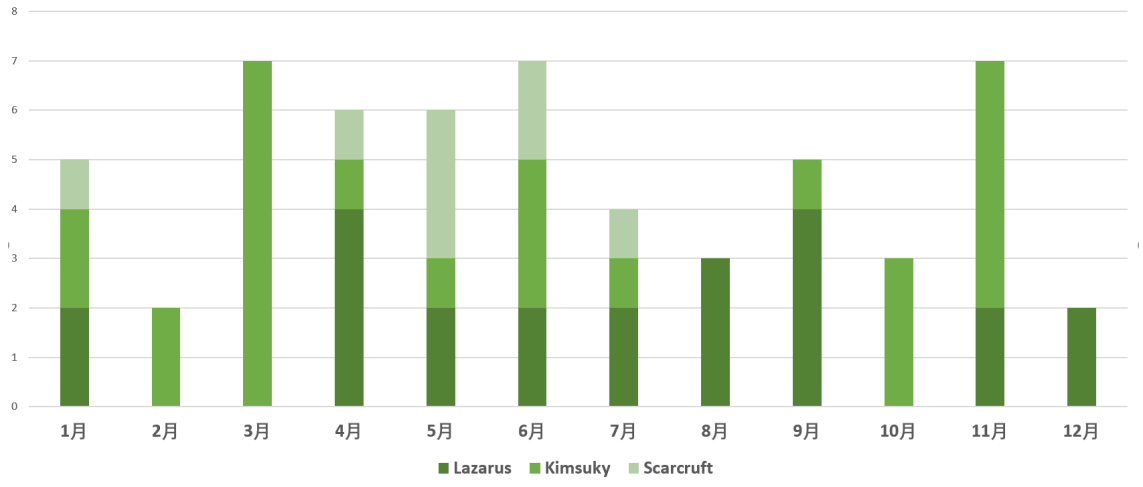
图3 响尾蛇APT使用阿富汗的国家安全委员会办公室相关题材的攻击文档

03 朝鲜半岛

Lazarus组织（APT-C-26）是朝鲜半岛非常活跃的APT组织之一，长期以数字货币、金融行业为攻击目标，通过网络攻击进行敛财。LAZARUS的多平台恶意框架MATA已对全球过个国家进行攻击，并获取目标用户的数据库信息，今年针对国内的“暴风行动”中发现该框架还被利用在攻击数字货币行业的攻击行动中。全球疫情爆发以来，lazarus集团还实施DreamJob行动[16]，通过社工攻击针对以色列及其他国家的国防、政府组织、企业的特定员工进行攻击，成功感染目标后收集相关财务状况的情报，可能是为了从中窃取钱财，这点非常符合Lazarus组织的一贯作风。

Scarcruft组织（APT-C-28），又名KONNI、Hermit、Group123、APT37。善于使用热点事件攻击，从2020年的攻击可以看出，主要以带有恶意宏的文档、HWP文档攻击。宏利用样本主要以核问题、网络安全、朝韩关系、政治时事、新冠疫情等话题为诱饵，文档中的宏代码出现了反复利用，同时还具有Android平台的攻击能力，实力不同小觑。

Kimsuky组织一直以来非常活跃，根据2020年的活动来看，攻击目标依旧聚集在韩国，今年疫情以来，多次利用新冠疫情、美国大选等国际热点话题等诱饵进行鱼叉式钓鱼攻击。近年也有相关研究证明Kimsuky和Scarcruft的攻击存在关联，他们在代码和网络资产上存在共享。



朝鲜半岛地区相关组织公开报告统计

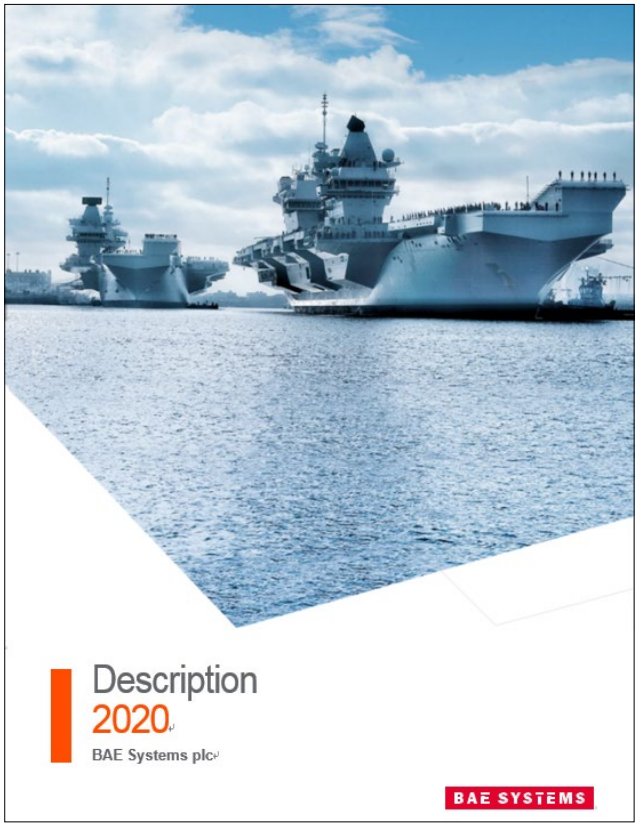
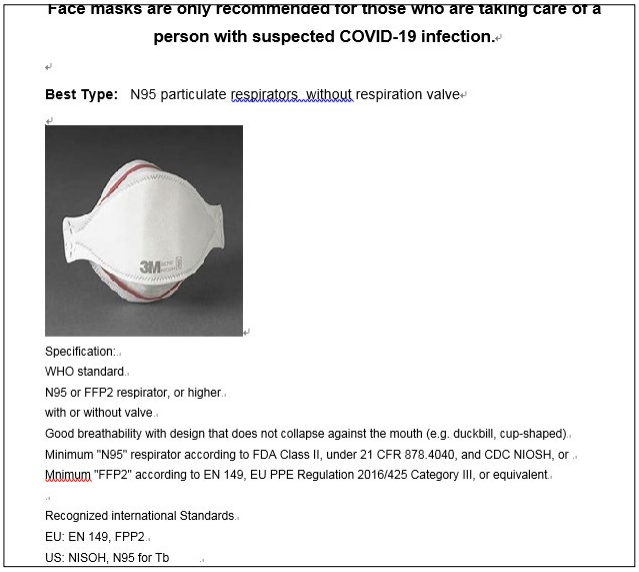


图1


Face masks are only recommended for those who are taking care of a person with suspected COVID-19 infection.

Best Type: N95 particulate respirators, without respiration valve

Specification:
WHO standard
N95 or FFP2 respirator, or higher
with or without valve
Good breathability with design that does not collapse against the mouth (e.g. duckbill, cup-shaped)
Minimum "N95" respirator according to FDA Class II, under 21 CFR 878.4040, and CDC NIOSH, or
Mnimum "FFP2" according to EN 149, EU PPE Regulation 2016/425 Category III, or equivalent

Recognized international Standards
EU: EN 149, FPP2
US: NISOH, N95 for Tb

图2

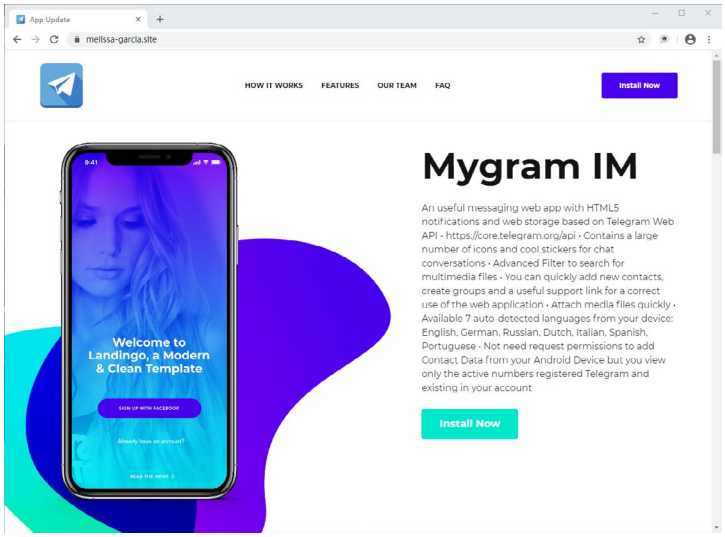
■ 图1 Lazarus组织MATA攻击中相关诱饵文档

■ 图2 Scarcruft组织以疫情口罩相关诱饵文档

04 中东地区

中东地区的APT攻击十分活跃，双尾蝎、Oilrig、Fox Kitten等组织都进行了多次攻击，针对目标多以政府、军事和能源相关。特别是APT34，即使去年三月份被泄漏了攻击武器库与攻击人员资料，仍然没有停止行动. Fox Kitten更是活动频频，从2019年至2020年通过多个VPN和网络设备的漏洞入侵企业网络。另外Crowdstrike安全厂商披露[17]，至少从2020年7月开始，Fox Kitten被发现在黑客论坛上出售其入侵企业的访问权限。

双尾蝎组织（APT-C-23），是一个针对中东地区相关国家的教育、军事等重要领域进行网络间谍活动，以窃取敏感信息为主的网络攻击组织。攻击平台主要包括 Windows 与 Android。该组织的攻击活动最早可追溯到2016年，近年来该组织活动频繁不断被数个国内外安全团队持续追踪和披露。



2020年2月16日，以色列国防军IDF网站称[18]，他们发现哈马斯的一系列网络攻击行动，通过制作了多个聊天工具相关的钓鱼网站，利用社交媒体伪装成美女诱骗以色列国防军士兵下载安装伪装成聊天工具的间谍软件，从而窃取以色列国防军的隐私信息，并最终认为与APT-C-23组织有关。5月，360烽火实验室发现了与以色列国防军曝光的双尾蝎组织攻击行动相关的另一起网络攻击活动[19]，该活动中使用的间谍软件伪装成MygramIM 应用，并利用钓鱼网站进行传播，根据网站信息，此次攻击活动仍然针对中东地区。

仿冒MygramIM应用钓鱼网站

传播分发方式还是以应用市场为常规渠道，如PhantomLance组织使用的主要传播媒介是通过应用程序市场进行分发[20]，为了能绕过Google Play的上架审查，其通常采用上架的初始版本不包含任何恶意代码，但在后续更新中再加入恶意代码。由于这种方式会增加随机感染的受害者，所以在双尾蝎后续新攻击中，不仅伪造了一个假的Android应用商店用于分发恶意软件，该应用商店中包含恶意应用以及正常合法的应用，但下载这些恶意应用时需要输入6位验证码，由此用以降低恶意软件的流行度，并更针对特定用户。

Domestic Kitten组织（APT-C-50）最早被国外安全厂商披露，自2016年以来一直在进行广泛而有针对性的攻击，攻击目标包括中东某国内部持不同政见者和反对派力量，以及ISIS的拥护者和主要定居在中东某国西部的库尔德少数民族。

2020年9月27日，亚美尼亚与阿塞拜疆之间存在领土争端多年，最近再次爆发了近年最严重的冲突。由于中东某国与冲突两国的共同边界，中东某国的角色和当局的决定对此次冲突来说非常敏感。或许为了防止可能对中东某国政权稳定构成威胁，我们观察到Domestic Kitten组织再次发起了攻击行动。

Domestic Kitten组织此次攻击活动[21]中使用了移动端攻击武器，伪装成居鲁士大帝和Mohsen Restaurant相关APP，从代码结构和功能上与商业监控软件KidLogger高度相似。我们在此次攻击活动中发现了一名活动在中东某国的疑似受害者，其可能参与了反政府相关活动。

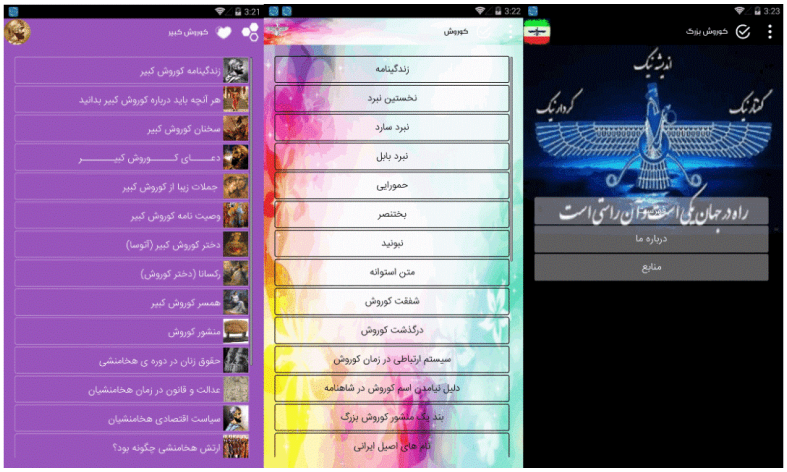


图1

图2

图1 恶意APP运行界面　图2 德黑兰-Af53-军事集中

05 其他

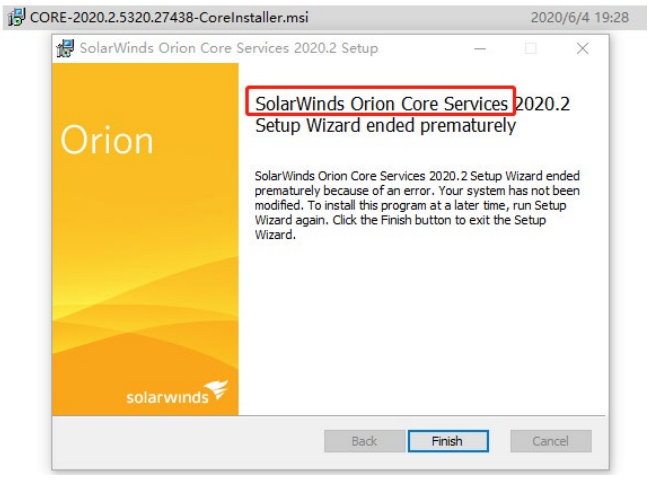
▪ UNC2452 (APT-C-54)

美国时间12月13日，SolarWinds公司Orion平台的多款软件被曝出植入了后门程序，该公司为全球30万家客户提供了产品服务。360第一时间对此安全事件进行了预警，将此次攻击行动命名为“落鹰行动”，并独家发布了此事件的完整揭秘分析报告。该公司疑似在2019年就被黑客组织入侵，控制了该公司核心软件的编译发布流程，在该公司软件的官方安装包和在线升级程序包中的核心服务组件植入了后门程序。

根据360安全大脑的全网安全数据分析，我们发现了SolarWinds供应链攻击事件中数百家组织机构的失陷信息，这些组织机构共涉及31个国家，其中美国失陷的组织机构最多。此外，涉及18个行业，其中政府组织机构失陷情况最为严重，其次是金融和IT行业，同时有少量网络安全公司。可以说，这是一场史上最严重的供应链攻击，致使全球数百家重要核心组织机构陷落，给安全业界敲响了长鸣的警钟。

◇ 攻击过程

攻击者在SolarWinds Orion平台软件2019.4 - 2020.2.1版本的核心服务组件 (SolarWinds.Orion.Core.BusinessLayer.dll) 中植入了恶意后门，该组件存在于SolarWinds的核心服务（SolarWinds Orion Core Services) 安装包和升级包内，该服务安装包又会打包进入所有Orion平台的离线软件安装包中，安装SolarWinds Orion平台的任意软件都会默认安装此服务。



SolarWinds Orion安装程序

我们在官方发布的2019.4 – 2020.2.1版本离线安装包、离线安装镜像和升级包中均发现了后门组件，被污染的后门DLL组件也都拥有合法的数字证书签名。因此可以推断攻击者已经控制了该软件的开发打包编译环节，软件在源代码层面就已经受到了污染，也就是说所有SolarWinds用户从任何渠道安装和升级的SolarWinds Orion平台软件都会被无差别的植入后门程序。其完整攻击流程如下图所示：

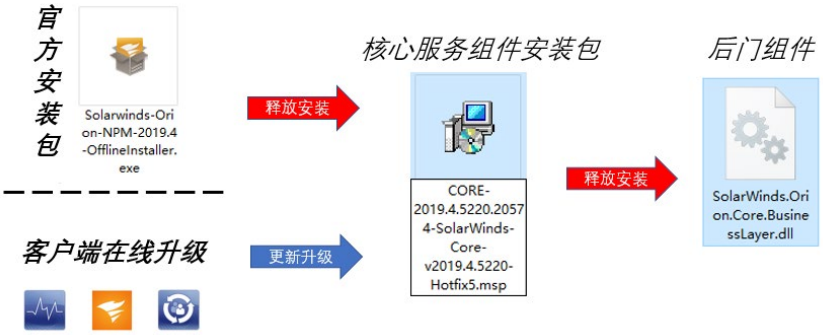


图1

◇ 攻击时间

根据360安全大脑的安全大数据，我们跟踪标注了SolarWinds后门组件（SolarWinds.Orion.Core.BusinessLayer.dll）的活跃时间，还原了“落鹰行动”的完整攻击时间轴，完整时间线如图所示。根据该组件的样本数据统计，“落鹰行动”的攻击时间最早可以追溯到2019年10月，甚至可能早于此时间。

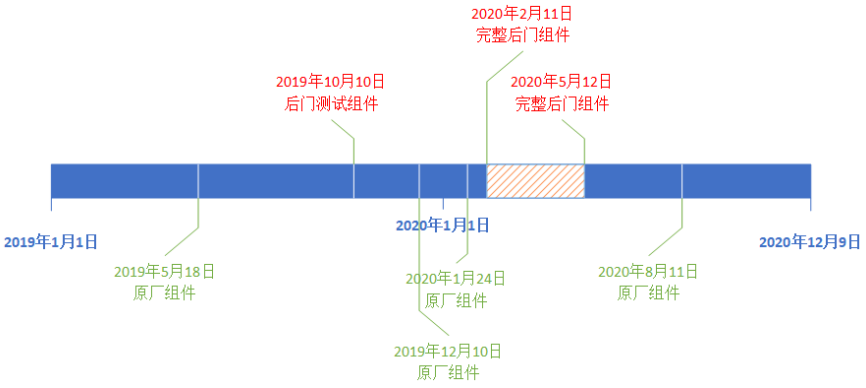


图2

■ 图1 针对SolarWinds Orion攻击流程　■ 图2 攻击活跃时间

2019年，攻击者初次在原厂组件中加入了名字为OrionImprovementBusinessLayer的后门类，其它正常原厂组件均无此后门类。值得注意的是，此后门类中初次置入的是一个环境变量判断的函数，我们推测攻击者是在进行第一阶段的后门测试验证。在经过测试验证后，攻击者在2020年实施第二阶段的正式攻击，在此后门类中正式加入完整的RAT代码，开始通过官方渠道对SolarWinds的客户植入后门程序。

攻击者第三阶段的攻击是针对目标的后渗透攻击，值得注意的是该类攻击进行了非常谨慎的安全对抗操作，如在C&C的DGA请求前做了大量的安全软件和工具检测，在DGA请求后对IP归属等进行了严格判断，因此失陷机构单独根据网络流量极难判断受损情况。

▪ Machete (APT-C-43)

9月，360安全大脑于国内首家追溯披露Machete (APT-C-43) 黑客组织[22]，并揭秘其行动极有可能是：为帮助胡安·瓜伊多领导的反动派窃取委内瑞拉军方的军事机密并提供情报支持而展开。因此，360安全大脑也将这一系列攻击行动命名为HpReact (译为：帮助反动派政府) 。而且截至目前，这些威胁活动仍然非常活跃。

在溯源过程中，研究员发现此次行动与APT组织Machete有所关联。而关于Machete，最早可追溯到2010年，该组织是一个具有西班牙语根源的APT组织，其攻击目标以拉丁美洲各国军事、使馆和政府机构为主。多年来，一直以收集目标国家情报并改进他们的攻击策略为目标。尤其是在2019年，外媒报道显示，有超过50台计算机被Machete攻击。约75%属于拉美各国的军事力量，其中一半以上属于委内瑞拉军队。与此同时，以GB为单位的机密文件和私人信息已被泄露到攻击者控制的服务器上。

值得注意的是，处于发展期的Machete组织，主要的后门也是基于Python编写的。而HpReact行动正是与Machete组织的情报窃取的行径相吻合。可以说，此次行动或为Machete组织在拉丁美洲从事网络战的冰山一角。

▪北非狐（APT-C-44）

10月披露，《北非狐（APT-C-44）攻击活动揭露》[23]。360烽火实验室联合360高级威胁研究院发现一起针对阿拉伯语地区的长达三年的多次网络攻击活动。该攻击活动自2017年10月开始至今，攻击平台主要为Windows和Android。通过分析，我们发现此次攻击活动来自北非地区，主要利用钓鱼网站和第三方文件托管网站进行载荷投递，并且使用社交媒体进行传播，受害者主要分布在阿拉伯语地区，其中包含疑似具有军事背景的相关人员。根据此次攻击活动的伪装对象和攻击目标，我们认为该组织目的是为了获取情报先机。根据该组织所属国家的地理位置以及其他特点，我们将其命名为北非狐（APT-C-44）。

2018年2月北非狐组织创建了一个Facebook账号用以传播恶意程序，该账号仿冒EgChat官方Facebook账号，后文中使用Fake EgChat表示仿冒账号。Fake EgChat主页与EgChat官方主页几乎一致（如下图所示），可见Facebook公司针对注册企业账号没有审核机制，正因如此，Facebook也成了APT组织传播恶意程序的常用渠道，此前我们揭露的黄金鼠组织同样使用了Facebook进行传播恶意程序。在Fake EgChat账号Facebook页面上可以发现所有的帖子均在传播钓鱼链接和恶意应用下载地址。其中的帖子最早可以追溯到2018年2月，并且至今仍然在更新相关钓鱼帖，如下图所示。

仿冒EgChat官方Facebook首页

PART 04

全球高级
持续性威胁 APT
研究报告

2020年攻击态势总结

01.针对我国的攻击较去年持续上升

360在过去数年发现了44个其他国家背景的高级黑客组织，监测到3000多次对中国的国家级网络攻击。2020年，360共披露了13个组织针对中国地区的攻击活动，其中4个组织是首次披露，如魔鼠、蓝色魔眼和旺刺等组织。今年境外APT组织针对我国相关机构或个人的攻击活动异常频繁，较去年持续上升，主要涉及我国政府、教育和国防军工相关单位。

从攻击趋势来看主要呈现出三个特点：

- 攻击频次显著上升

首先攻击频次增加，南亚、东南亚和东亚的APT组织最为活跃，其中蔓灵花、响尾蛇攻击范围和投入的资源几乎是去年的一倍；

- 攻击范围拓展扩增

其次是攻击目标领域有所拓展，除了受新冠疫情影响导致医疗行业备受APT组织的关注，另外还出现其他目标范畴的拓展，如海莲花组织今年集中针对国内多个软件服务商的供应链攻击，和侧重关注教育领域都是以往鲜有的。

- 新组织不断涌现

最后是针对中国地区的攻击以如海莲花、白金等已知组织的新攻击活动为主，但也出现如蓝色魔眼、魔鼠等多个历年来以国际战场为主的APT组织，今年针对中国的攻击也尤其活跃。

02.新冠肺炎疫情全球化对APT的影响

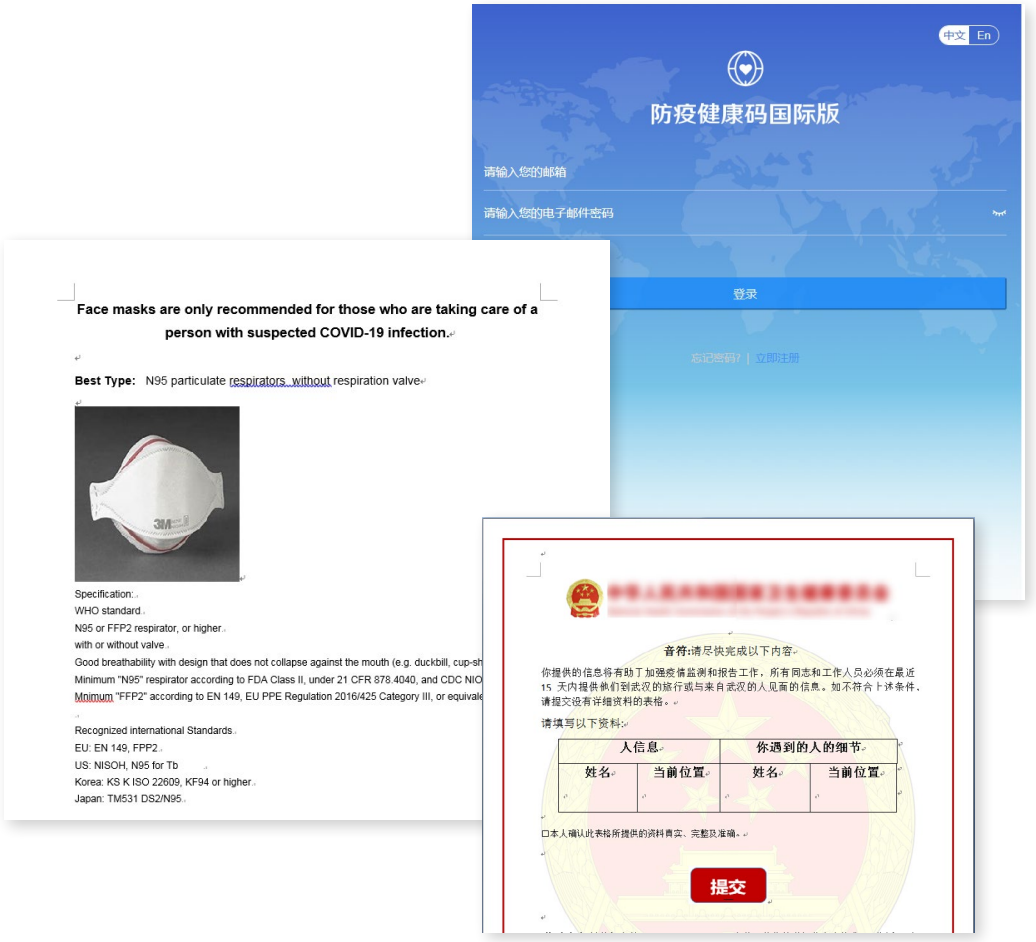
2020年初，在新冠疫情给全球格局带来新的冲击影响下，境外APT组织针对我国的攻击活动年初即开始激增，通过对全年攻击的研判分析，我们发现疫情对APT的影响主要体现在三个方面。

1.围绕“新冠肺炎疫情”话题的诱饵钓鱼最为活跃

利用疫情作为诱饵信息，如“新冠肺炎“、”COVID-19“等关键词在诱饵文档、钓鱼网站等攻击中频繁出现。以围绕新冠疫情话题的利用攻击已成为今年最频繁的诱饵信息，随着疫情在国内的有效控制，此类攻击也从突增爆发逐步转为常态模式，但由于近期全球确诊已突破9000万，随着冬季到来，疫情可能再度迎来高峰等变化，相关利用攻击也开始出现小范围突增；

诱饵文档文件名
XXX传防发文件
XXX中心工作通知
新型冠状病毒感染引起的肺炎的诊断和预防措施
新冠肺炎防控内部参考手册
武汉旅行信息收集申请表
武汉肺炎
我国新型冠状病毒疫苗临床研究进展
XXX指令
收集健康准备信息的申请表
冠状病毒实时更新：中国正在追踪来自湖北的旅行者
kreab china report on covid 19 impact challenges and opportunities Covid19_Guidelines

2020年攻击活动中围绕“新冠肺炎疫情”部分诱饵文档文件名



2.针对医疗行业的攻击明显上升

4月23日，世卫组织发表声明称[24]，自新冠肺炎疫情开始以来，针对世卫组织的网络攻击数量急剧增加，是去年同期的五倍多。世卫称，发布声明这周约450个活跃的电子邮件地址和密码被泄露，还有数以千计的研究人员邮件信息被泄露。基于360安全大脑监控数据显示，针对医疗行业的威胁不仅在传统网络攻击大量出现，APT针对性攻击也出现明显增长，尤其在今年第一季度新冠疫情初期尚未完全控制的期间。

今年针对医疗行业的攻击明显上升，如年初南亚CNC组织针对我国某医院和医科大学的定向攻击，2月中旬海莲花组织针对我国某医疗机构的集中攻击等，近期我们还捕获到一境外未知组织针对医疗器材行业的攻击活动，其中涉及多个单位受影响。但从整体攻击领域来看，APT组织还是更多聚焦政府、国防军工等领域，针对医疗行业的攻击或许只是短期阶段性目标；

2020年攻击活动中围绕“新冠肺炎疫情”部分诱饵文档或钓鱼页面内容

3.远程办公成为APT攻击“众矢之的”

今年春节复工后，有3亿多用户使用远程办公，远程办公在复工30天内环比上升了663%。据中国信通院抽样调查结果，九成信息消费企业采取“远程办公为主、驻地办公为辅”的开工模式。全球化的远程办公让攻击者更好的有的放矢，鱼叉邮件攻击由此达到事半功倍的效果。进一步基于远程办公基础设施的攻击成为关键，今年4月披露的Darkhotel组织利用某厂商VPN 0day、某厂商OA系统漏洞针对我国重要政府机构的攻击，以及7月揭秘的魔鼠组织利用同一厂商VPN漏洞发起定向攻击等。

CVE	产品	漏洞类型	补丁时间
CVE-2020-16875	Microsoft Exchange Server	远程执行代码漏洞	09/08/2020
CVE-2020-17085	Microsoft Exchange Server	拒绝服务漏洞	11/10/2020
CVE-2020-17084	Microsoft Exchange Server	远程执行代码漏洞	11/10/2020
CVE-2020-17083	Microsoft Exchange Server	远程执行代码漏洞	11/10/2020
CVE-2020-17143	Microsoft Exchange	信息泄露漏洞	12/08/2020
CVE-2020-17141	Microsoft Exchange	远程执行代码漏洞	12/08/2020
CVE-2020-17117	Microsoft Exchange	远程执行代码漏洞	12/08/2020

03.物联网设备-APT新的战备资源

1.国家安全机构建物联网僵尸网络

今年3月，疑似东欧黑客组织“数字革命”曝光了一份代号为“Fronton”的项目文档[25]，该项目文档描述了承包商如何建立物联网僵尸网络的细节。

通过项目文档的架构图，我们可以一窥该僵尸网络的架构细节，幕后人员通过多重VPN网络和TOR网络控制着主要由网络视频录像和网络视频监控等物联网设备构建的僵尸网络

当僵尸网络掌控着数以百万计与互联网连接的网络设备后，相关组织机构也就掌握了相应规模的网络攻击资源，幕后人员利用这些设备的计算能力和带宽流量可以发起惊人破坏力的DDOS攻击，也可以提供海量的跳板代理资源帮助APT攻击活动隐蔽行踪。

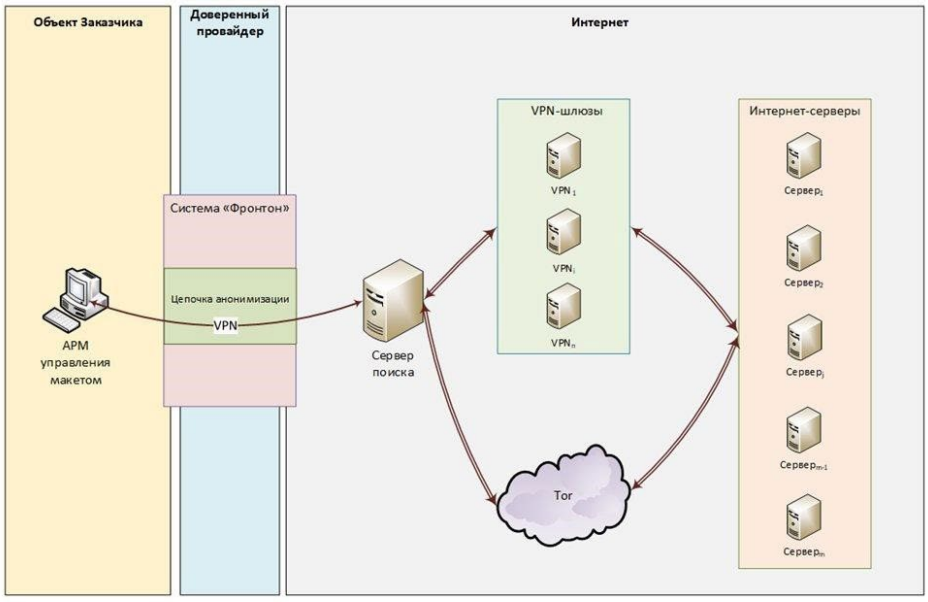


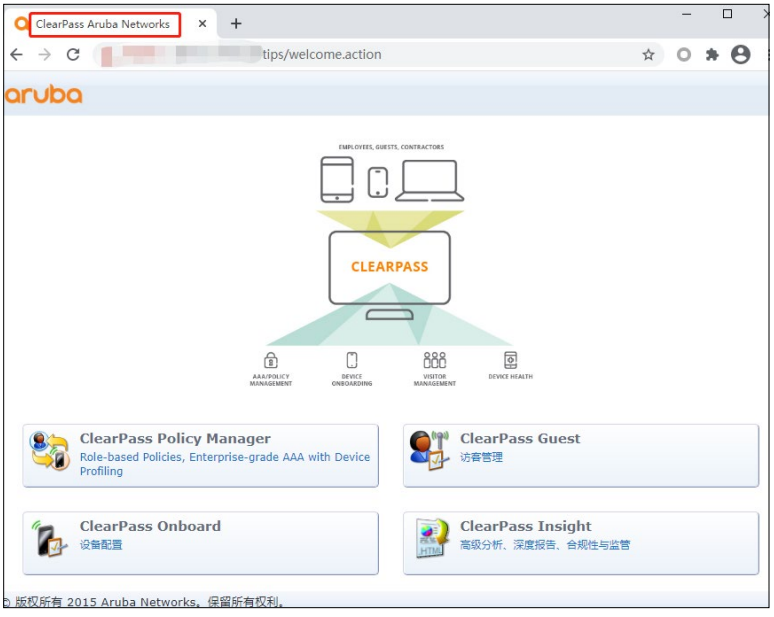
Рис. 1. Структурная схема макета

2.Lazarus组织针对Aruba网络设备的攻击活动

我们观察到今年Lazarus组织出现针对linux平台攻击的变化趋势，该组织的攻击开始向物联网设备伸出魔爪，以物联网设备作为入侵目标的突破口，进一步对目标实施以网络勒索为目的的入侵渗透。

360高级威胁研究院在今年10月发现Lazarus组织首次针对Aruba网络设备发起了攻击活动，攻击目标涉及Aruba公司的产品，Aruba公司主要为金融、政府、医疗、教育、零售、酒店等行业提供网络接入和管理的产品解决方案。

基于攻击活跃的时间节点往前推移，我们注意到Aruba ClearPass Policy Manager平台在9月被曝光了一个远程命令植入漏洞 (CVE-2020-7115) 的技术细节[26]，而失陷目标大部分都对外开放了Aruba ClearPass服务入口。攻击者疑似是此漏洞细节曝光后，在网络空间中搜索存在安全漏洞的Aruba设备实施了大规模攻击。我们发现本次攻击活动在欧美、亚洲等多个国家都受到了影响，主要涉及高校、能源和医疗等行业。



对外开放的Aruba ClearPass服务入口

04.供应商演变成全行业的安全短板

供应链攻击并不是什么新兴攻击手法，早在2015年就有苹果应用程序编译器Xcode被植入恶意代码的XcodeGhost事件[27]，2017年NetSarang旗下Xshell软件的关键模块被植入高级后门的XshellGhost事件[28]，2019年华硕ASUS Live Update更新服务被植入木马的供应链攻击事件[29]等等。

近年来引起业界轰动的供应链攻击安全事件一直不绝于耳，一遍一遍在敲打着业界这座看似坚固实则脆弱不堪的安全城墙。2020年供应链攻击的安全事件并没有消停，供应商的安全问题造成影响全行业的安全危机事件一件一件被披露。我们看到信息安全的“木桶理论”放到行业层面也是适用的，整个行业上下游的木板组成了行业的信息安全木桶，一家公司的安全问题所造成的危害绝不仅仅只影响自身，还可能会演变成全行业陷落的安全短板。

1.国内多起APT供应链攻击事件

360安全大脑今年捕获多起供应链攻击事件，涉及海莲花、Darkhotel等多个组织。对外披露了两起基于供应链的APT攻击事件，APT组织均针对目标单位的供应商作为攻击行动的突破口，利用供应商的安全漏洞和服务资源大范围攻陷目标单位。

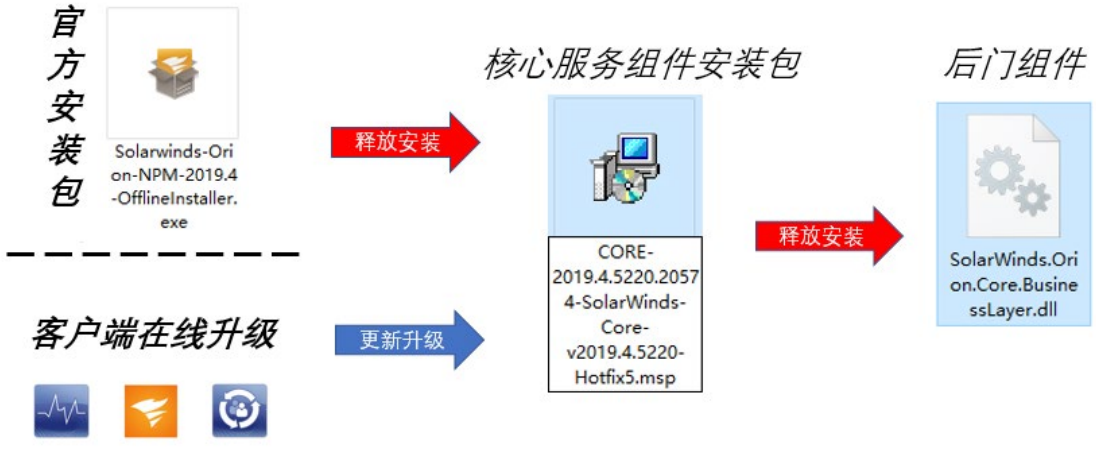
今年4月，360独家捕获了DarkHotel组织利用某厂商VPN服务器的升级漏洞针对我国政府机构进行的定向攻击行动，该组织利用VPN客户端更新过程中的一个0day漏洞，用后门程序取代了合法的升级更新程序，受害机构有超过200台的VPN服务器被植入了后门程序。

今年7月，美国网络安全与基础设施安全局（简称CISA）[30]和360先后披露了WellMess组织的APT攻击活动。根据360的披露，该组织实施了相对复杂的供应链攻击，从2018年开始就针对多个目标单位的同一邮件系统供应商发起了定向攻击，利用DarkHotel组织类似的攻击手法针对邮件系统供应商的售后、运维人员发起了攻击，在利用攻陷供应商相关售后维护途径入侵至客户的内网，受影响的目标单位涉及科研、通信等组织机构。

2.史上最严重的供应链攻击

美国时间12月13日，SolarWinds公司Orion平台的多款软件被曝出植入了后门程序，该公司为全球30万家客户提供了产品服务。360第一时间对此安全事件进行了预警[31]，并独家发布了此事件的完整揭秘分析报告，该公司疑似在2019年就被黑客组织入侵，控制了该公司核心软件的编译发布流程，在该公司软件的官方安装包和在线升级程序包中的核心服务组件植入了后门程序。

根据360安全大脑的全网安全数据分析，我们发现了SolarWinds供应链攻击事件中数百家组织机构的失陷信息，这些组织机构共涉及31个国家，其中美国失陷的组织机构最多。此外，涉及18个行业，其中政府组织机构失陷情况最为严重，其次是金融和IT行业，同时有少量网络安全公司。可以说，这是一场史上最严重的供应链攻击，致使全球数百家重要核心组织机构陷落，给安全业界敲响了长鸣的警钟。



针对SolarWinds Orion攻击流程

05.针对移动平台的APT攻击持续活动

当前手机已经成为各类信息系统的连接中心，从我们今年发布的报告可以明显看出，越来越多的APT组织正在参与开发针对移动设备的植入工具。APT组织在移动端执行攻击活动中，通常采用WhatsApp消息，短信，应用市场和社交媒体作为初始感染媒介。相比PC端，这些作为移动端常见的攻击入口，通过文字描述和诱饵图片，更容易诱导攻击目标点击包含恶意软件的下载链接。4月，我们在肚脑虫组织（APT-C-35）攻击活动中发现攻击样本存在于WhatsApp应用软件目录下，根据巴基斯坦信德省官方网站公布的一份报告中显示[32]，该组织通过WhatsApp社交软件对巴基斯坦武装部队和巴基斯坦三军情报局相关人员发起了一系列网络攻击活动。10月，我们在Facebook上仿冒EgChat 账户的页面信息里，发现了北非狐（APT-C-44）使用的恶意软件下载链接。当然，应用市场仍然是常规的传播分发方式，PhantomLance组织使用的主要传播媒介是通过应用程序市场进行分发，为了能绕过Google Play的上架审查，其通常采用上架的初始版本不包含任何恶意代码，但在后续更新中再加入恶意代码。由于这种方式会增加随机感染的受害者，所以也出现了双尾蝎（APT-C-23）组织使用伪造的应用市场，使用特定验证码的方式来下载，用以降低恶意软件的流行度，增加攻击目标的针对性。

在初始入侵阶段，除了感染媒介，为了欺骗攻击目标下载安装恶意软件，今年我们还看到APT组织精心设计的不同类型钓鱼网站。2月，以色列国防军指责哈马斯策划“蜂蜜陷阱”行动诱使以色列国防兵下载伪装成多个约会应用程序的移动远程访问木马，这些伪装的约会应用程序背后都拥有一个看似官方的独立网页，提供软件介绍和下载服务支持。10月，我们发现北非狐（APT-C-44）组织曾经在2017年制作了一个仿冒EgChat官网的钓鱼网站EgChaat，钓鱼网站界面与官方网站只有极少的差异。同月，我们还发现肚脑虫组织（APT-C-35）仿冒了一个在巴基斯坦流行的在线交友网站LoveHabibi。

在仿冒应用软件方面，4月底印度军队发出警告[33]，警告Transparent Tribe透明部落组织正在借助COVID-19全球大流行，仿冒印度政府电子和信息技术部下属的国家信息中心开发的COVID-19跟踪应用软件，用来入侵印度军事人员的手机。另外其他组织伪装的对象比如居鲁士大帝、斋月、锡克教分离主义运动等，针对特定的宗教和政治团体。

06.APT组织与安全机构对抗愈发激烈

APT组织与安全机构的对抗，并非只停留在传统攻击对抗中恶意代码主要以躲避、绕过等策略。有效的事先识别和不涉足安全防御体系的视野，是APT组织发起一次攻击中最基本的原则策略，如落鹰行动针对Solarwinds攻击中，一旦发现如卡巴斯基、CrowdStrike、FireEye等安全产品，则会关闭相关服务使之安全防护能力失效。

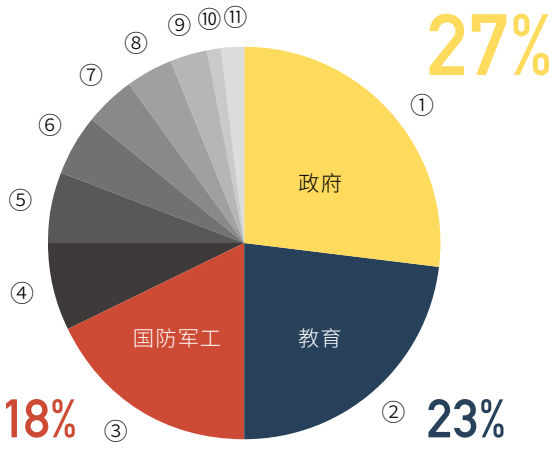
另一方面APT组织还会善于利用目标环境内的安全防护措施，事其变为攻击中的跳板或“敲门砖“，如当突破边界到达用户内网环境，会利用杀软软件产品进行进一步的横向移动。这主要取决于此类安全类产品本身内网覆盖高、突破传统隔离阻断等特性。今年捕获到的海莲花、Darkhotel等组织都有利用。

当然有些APT组织的攻击意图并不仅局限于此，安全机构厂商才是他们最终目标，当然这也不是新的发展趋势，如早期的卡巴斯基安全厂商被duqu2.0攻陷[34]。今年3月疑似东欧某政府机构承包商被入侵，导致有关入侵物联网 (IoT) 设备的Fronton项目细节被泄露。12月初FireEye安全厂商被攻击导致其红队安全工具被泄露[35]。

07.关键行业分析

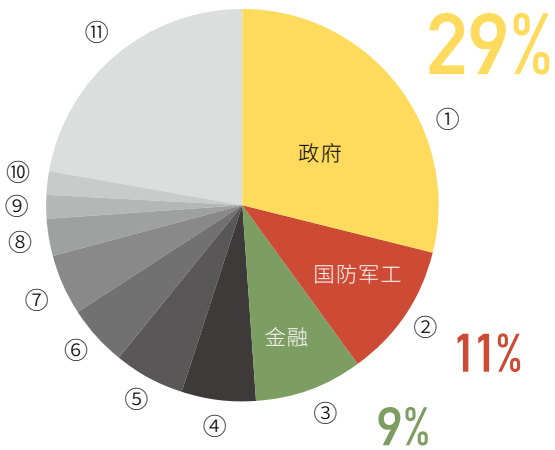
政府、国防军工、科技一直以来都是APT攻击的主要领域，由于国家背景因素，几乎所有APT组织都会关注着几个领域。但由于攻击意图的不同，各组织之间针对行业的差异较大。我们发现北美等地区技战术攻击手法复杂且战备资源充足的组织，针对的行业或单位都相对单一且更聚焦持久，而南亚、东亚等地区攻击能力偏弱的组织则与之相反。

除以上相关领域之外，金融、能源、通信和医疗也是今年APT攻击的主要领域，尤其是新冠肺炎疫情的影响下，医疗行业的威胁更加凸显。本章节会对相关领域今年涉及的攻击和影响展开介绍。



①政府 27%
②教育 23%
③国防军工 18%
④IT供应商 7%
⑤通信 6%
⑥科研 5%
⑦能源 4%
⑧医疗 4%
⑨贸易 3%
⑩金融 1%
⑪其他 2%

图1



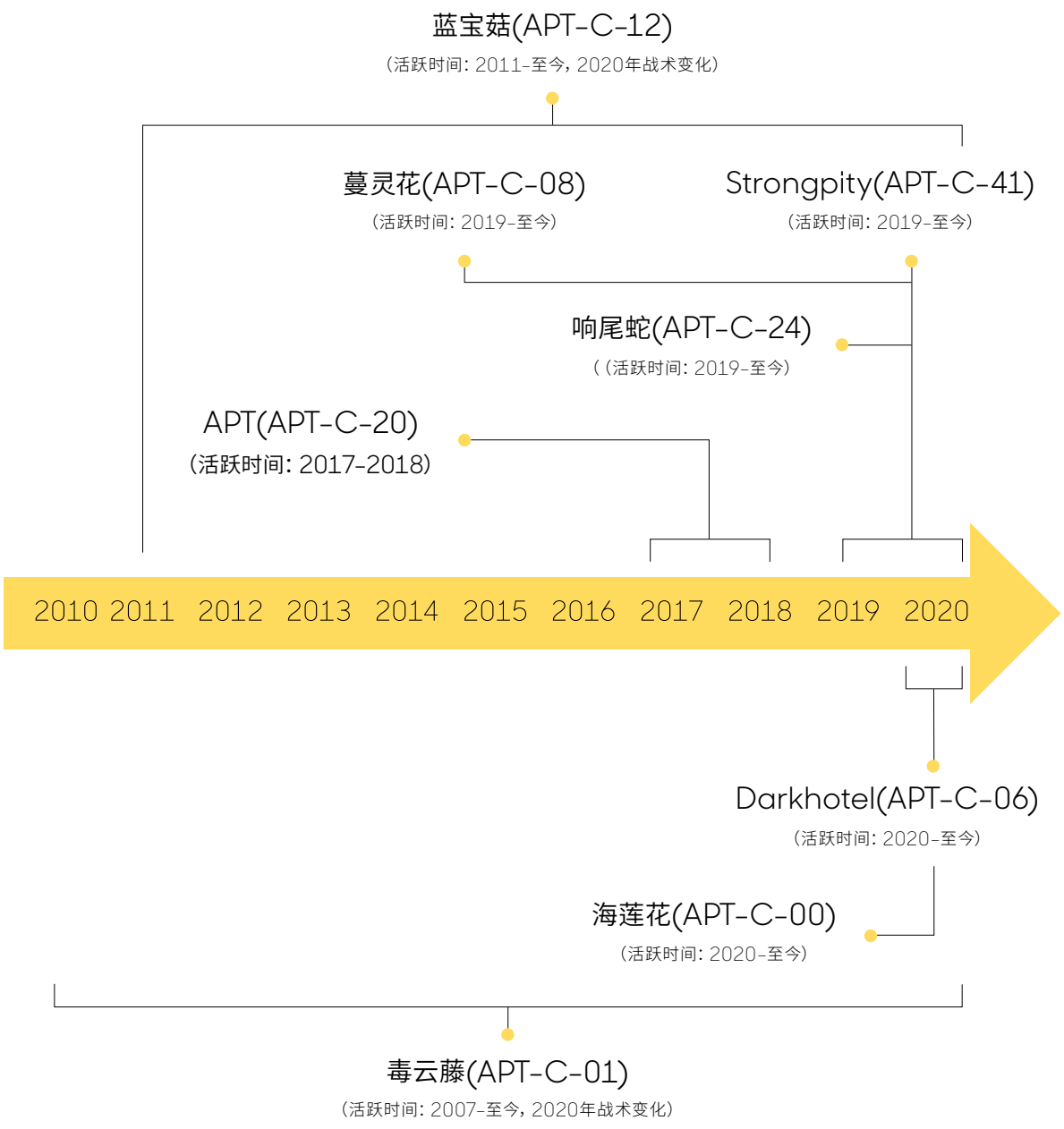
①政府 29%
②国防军工 11%
③金融 9%
④医疗 6%
⑤科研 6%
⑥能源 5%
⑦教育 5%
⑧航空 3%
⑨媒体 2%
⑩制造业 2%
⑪其他 22%

图2

■ 图1 2020年中国地区受影响行业分布 ■ 图2 2020年公开APT报告涉及行业分布

1.军工

在新冠疫情、国际关系日趋复杂等多种因素影响下，2020年境外APT组织针对我国军工行业的攻击非常活跃。历年来我国军工行业相关单位都是被APT组织的攻击重点目标，相关攻击最早可追溯到2007年，涉及的境外APT组织众多，主要活跃的组织如下图：



涉及国内军工行业主要活跃组织

▪ 围绕军工行业的攻击愈发频繁且针对性更强

境外APT组织针对我国军工行业的攻击活动长期持续且逐渐活跃，早期以早期APT组织为代表的攻击均直接攻击重点军工目标单位，且一旦突破边界继展开长期潜伏和横向渗透攻击，相关攻击往往会对某具体单位造成重大且持续影响。而东亚APT的攻击活动更倾向针对军工行业相关联的科技机构、高校、供应链单位等，常以军工展会、军民融合等为主题进行定向攻击，通过迂回战术来达到窃取军工行业机密情报，但从2020年开始东亚相关APT组织相关作战策略也开始升级调整，直接针对重点军工单位的攻击也愈发频繁，我们推测攻击者当前急于直接攻击，也有可能由于今年台海局势逐渐升级有关。

2020年初开始，以往针对军工行业采取保守蛰伏状态的多个APT组织突然开始活跃，其中主要包括南亚、中东等相关APT组织，其中以蓝色魔眼（APT-C-41）、蔓灵花（APT-C-08）、响尾蛇（APT-C-24）最为活跃。

▪ 航空、船舶工业是重点被攻击领域

不同APT组织针对的具体军工单位目标会有一定差异性，整体而言其中以航空工业、船舶工业影响最严重，这两个领域也基本是相关APT组织都会涉及到的。strongpity和APT28等组织都是以航空工业作为重点攻击目标。而在针对军工行业相关细分领域这方面，南亚APT组织在初始攻击刺探期间基本都会涉及。

▪ 南亚APT组织是主要攻击来源

基于相关APT组织近两年的攻击活动分析得出，从相关攻击带来的实际影响范围和持续时长来评估，南亚APT组织是主要攻击来源。但从今年开始南亚组织的攻击开始频繁活跃。

中东APT组织蓝色魔眼今年开始很活跃且主要聚焦航空工业，其他Darkhotel、海莲花、毒云藤、蓝宝菇等老牌APT组织今年也是积极活跃，造成的实际影响和持续时长较南亚APT组织还较弱，但如果按现阶段的聚焦性和发展趋势，有可能未来一段时间会造成较大影响。

2.金融

金融是国家重要的核心竞争力，21世纪全球金融化发展趋势决定了中国必须更加强调金融的重要性，防范系统性金融风险和提防外部金融冲击是关系国家安全的大事，有效防范系统性金融风险，必然要求建立健全制度行的监管机制。除了现有的制度的建立，网络的快速发展，从最初的金融诈骗到数字货币中，由国家级发起的攻击行动，可能引发更为严重的影响。近几年境外APT组织或境内组织以APT攻击手法针对金融行业的渗透，相关攻击事件陆续浮出水面。针对这类高级威胁，如何加强排查和防范是金融行业，尤其如数字货币这类新兴领域的艰巨挑战。

Lazarus组织已从传统金融领域战场转移到数字货币等新兴领域，从2015年开始活跃于银行ATM、SWIFT攻击，逐渐到勒索敲诈、数字货币相关攻击，尤其今年针对数字货币领域的攻击异常活跃。近几年，以Lazarus为代表的境外APT组织持续对金融领域攻击渗透，从聚焦于数字货币监管机构、交易所等人员进行精准定向攻击，到根据不同岗位不同资源目标人群，采取差异化攻击手段，进而达到窃取交易所相关数字资产，甚至更为核心机密资料的目的。

早在2017年全国金融工作会议上，习总书记就强调，金融是国家重要的核心竞争力，金融安全是国家安全的重要组成部分。伴随全球信息化、数字化的发展，针对金融领域以及数字货币行业觊觎与攻击，也成为国家级网络力量博弈的一重要领域。尤其当前，正值我国大力推进数字货币关键时期，相关政策方向、技术突破等都将成为APT组织幕后主导者重点关注所在。

活跃时间	攻击行动	针对目标
2019年8月至2020年9月	暴风行动	伪装交易平台，针对交易所人员
2018年3月至2020年11月	危险密码[36]	投递诱饵文档，针对数字货币行业
2020年4月至2020年11月	CRAT[37]	投递诱饵文档，针对数字货币行业

2020年Lazarus针对数字货币主要的三次攻击活动

另外值得关注的是针对全球范围内金融行业情报窃取的DeathStalker组织，该组织以及涉及的Evilnum家族的相关攻击活动，今年卡巴斯基[38]、ESET[39]等多家安全厂商进行了披露曝光。该组织攻击范围仅限于全球范围金融行业、律师事务所领域，相关攻击活动最早可以追溯到2012年。其中涉及Evilnum家族的攻击最为活跃，值得注意的是该组织并不是直接窃取用户资金财产、不会部署勒索软件或从事传统金融犯罪黑产活动，其主要目的是窃取所关注企业的商业敏感数据。攻击手法主要以伪装为交付单、投资汇报文件、信用卡信息或公共服务账单等。


swisscom

Rechnung

Panagiotis Karaiskos
Im Spitz 5
8304 Wallisellen

Rechnungsbetrag	CHF 105.00
Zahlbar bis	29.09.2020
Rufnummer	044
Datum	04.(
Rechnungskonto	BSC 44
Rechnungsnummer	770 020
Kundennummer	481
Rechnungsreferenz	1.2(

Ihre Rechnung August 2020

	Betrag
Abonnemente	105.00
Rechnungsbetrag inkl. MWST in CHF	105.00

Ist Ihre Website bereits verschlüsselt?

Schützen Sie sich und ihre Kunden vor Datenklau und wechseln Sie jetzt zu Swisscom Webhosting oder HomepageTool.

3.能源

针对我国能源领域相关重点单位，一直是境外APT组织长期重点关注目标，近几年以东南亚和东亚的组织为主。今年持续活跃最有代表性的是海莲花和Darkhotel这两个老牌APT组织，而另外响尾蛇、毒云藤等多个APT组织针对该领域均有阶段性攻击活动，但并未持续活跃。海莲花组织长期针对我国政府、能源、科研等重要机构，今年涉及石油行业相关单位的攻击频繁。Darkhotel组织更多针对电力行业重点单位，采用最新thinmon攻击组件。

伪装瑞士电信账单

2020年以来，全球范围内先后发生了多起针对能源行业的攻击事件，造成了严重的影响。1月，APT33组织攻击欧洲能源部门[40]，此次攻击旨在窃取与欧洲能源相关的敏感信息；4月，思科Talos披露发现有针对阿塞拜疆能源领域的攻击[41]，主要是与风力涡轮机相关的SCADA系统；今年9月，Zscaler安全团队披露了针对中东石油和天然气行业多个供应链组织的攻击活动[42]，主要通过钓鱼邮件的方式传播恶意PDF文件。

作为关系国家安全和民生的关键信息系统，能源行业的网络安全风险所带来的不仅仅是信息泄露、信息系统无法使用等“小”问题，而是会对现实世界造成直接的、实质性的影响，如社会生产瘫痪、交通瘫痪、设备损坏、环境污染等。

发布时间	攻击事件	发布机构
1月23日	APT33攻击欧洲能源部门	Recorded Future
1月7日	伊朗APT组织入侵沙特石油公司	prevailion
4月14日	葡萄牙跨国能源公司（天然气和电力）EDP遭勒索软件攻击，赎金高达1090万美金	bleepingcomputer
4月16日	思科Talos披露发现有针对阿塞拜疆能源领域的攻击，主要是与风力涡轮机相关的SCADA系统	思科Talos
7月2日	6月16日巴西的电力公司Light S.A被黑客勒索1400万美元的赎金，AppGate的安全研究人员分析认为是Sodinokibi勒索软件	securityweek[43]
9月29日	对中东石油和天然气供应链产业的针对性攻击	Zscaler
11月20	10月12日，印度孟买遭受大规模严重断电事件，疑似源自国家支持的黑客攻击活动。	businessinsider[44]

2020年针对能源行业主要攻击事件

Request for Quotation ("RFQ")

Date: 29-Aug-2020

RFQ Title: PI-18031: Dalma Gas Development Project (Package B)-TENDER BULLETIN-01

BIDDERS SHOULD DOWNLOAD THE TECHNICAL AND COMMERCIAL RFQ FILES FROM BELOW AND ARE ADVICED TO MAINTAIN THE FORMAT WHILE MAKING QUOTATION

TECHNICAL AND COMMERCIAL FILES:

PROJECT DESCRIPTION FILE
https://we.tl/t-cFvm5QQlyV
COMMERCIAL FILE 01-02: BOQ, SPECS. & DRAWINGS
https://we.tl/t-nMKuKWbMlE
STEPS TO ALLOW DOWNLOAD FROM CHROME BROWSWER IF YOU ARE BEING BLOCKED FROM DOWNLOAD:

1. In the top-right corner of the browser window, click the Chrome menu Chrome menu.
2. Select Settings.
3. Click Show advanced settings.
4. Under "Privacy," uncheck the box "Protect you and your device from dangerous sites"

For and on behalf of Abu Dhabi Oil Refining Company

For Procurement Division

4.通信

从早期的美国国家安全局NSA旨在监视全球手机网络发起的代号为AURORAGOLD（极光黄金）计划被披露[45]，到去年MuddyWater组织针对伊拉克移动运营商（Korek Telecom）发起的定向攻击[46]和DeadlyKiss[47]全球范围针对基础电信行业的攻击。从这些重大攻击事件、幕后背景和影响广泛程度等，我们不难看出通信行业，尤其是基础电信行业对这些具有国家背景APT组织的重大战略意义。

新冠疫情影响下全球化的远程办公、云上作业等，使得今年通信行业面临的问题挑战和相应而来的威胁较以往都更加严峻。基于360安全大脑对APT组织攻击活动的持续监控，我们发现今年针对通信行业的攻击活动依然很活跃，虽然攻击涉及APT组织不多，但相关攻击呈现短期集中频繁且潜伏时间极长。

海莲花（APT-C-00）老牌APT组织，从去年年底开始将通信行业相关单位作为重点攻击目标，该组织今年技战术整体都有较大调整提升，针对通信行业的攻击也采用了最新的供应商攻击方式。潜行者（APT-C-30）是一个长期针对我国重点政府、通信等领域，来自东南亚方向的组织，该组织以攻击行动隐蔽低调，攻击周期长为特点，涉及我国通信行业的攻击最早可以追溯到2014年，尤其今年针对某基础电信企业的攻击非常活跃。

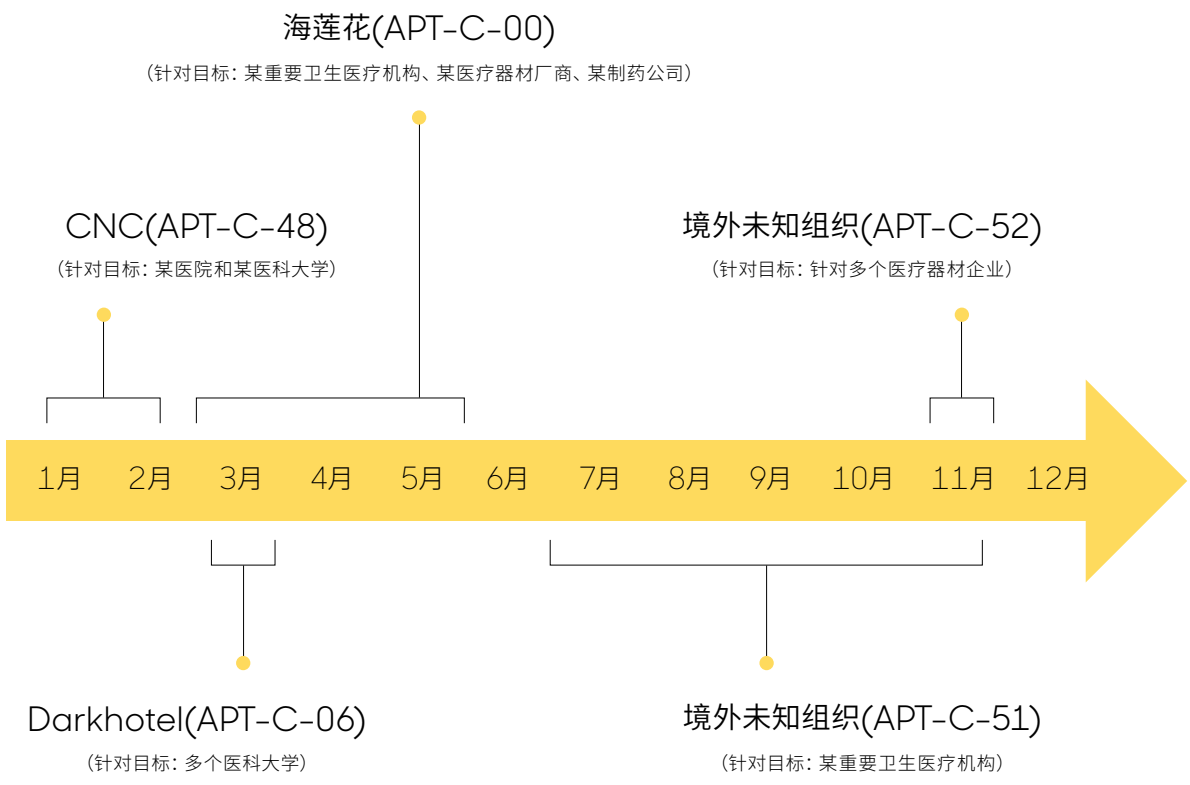
虽然今年针对基础电信行业的APT攻击还是以网络间谍窃密为主，但针对通信行业涉及劫持破坏等威胁还需要持续重点关注，如今年发生的俄罗斯电信运营商Rostelecom劫持事件[48]、阿根廷电信公司遭受勒索软件攻击，这些攻击无论是过失、趋利或其他意图，这种危及到核心业务本身，所造成的实际影响是巨大的。

5.医疗

4月23日，世卫组织发表声明称[49]，自新冠肺炎疫情开始以来，针对世卫组织的网络攻击数量急剧增加，是去年同期的五倍多。世卫称，发布声明这周约450个活跃的电子邮件地址和密码被泄露，还有数以千计的研究人员邮件信息被泄露。基于360安全大脑监控数据显示，针对医疗行业的威胁不仅在传统网络攻击大量出现，APT针对性攻击也出现明显增长，尤其在今年第一季度新冠疫情初期尚未完全控制的期间。

CNC组织主要在年初国内疫情爆发期间，主要针对我国某医院和医科大学的集中攻击，攻击者利用肺炎疫情相关题材作为诱饵文档（如：武汉旅行信息收集申请表），通过邮件投递攻击。2020年1月末，我们立即对相关重点客户进行预警加强防范，从2月初开始该组织相关攻击已经收敛缓解。2月下旬又监控发现源于东南亚的海莲花组织，针对我国某重要卫生医疗机构、医疗器材和制药公司等多家单位，其最终意图是为了窃取相关抗疫机密情报信息，相关攻击持续到5月。另外今年东亚方向的Darkhotel、毒云藤组织也积极活跃在我国多家医科大学、制药公司等。进一步下半年我们监控捕获到两个境外未知组织，分别针对国家重点医疗机构和医疗器材行业展开针对攻击。

由于全球疫情并非能一朝一夕完全结束，未来针对医疗行业的威胁会持续高于以往，但从整体攻击态势和涉及领域来看，APT组织更多还是借助新冠疫情热点话题，来聚焦政府、国防军工等领域。针对医疗行业的攻击或许只是阶段性目标，另一方面随着远程医疗等新攻击面的产生，以及类似以勒索为手段，而目的是破坏的攻击频发，我们不仅不能掉以轻心还需进一步加强警惕。



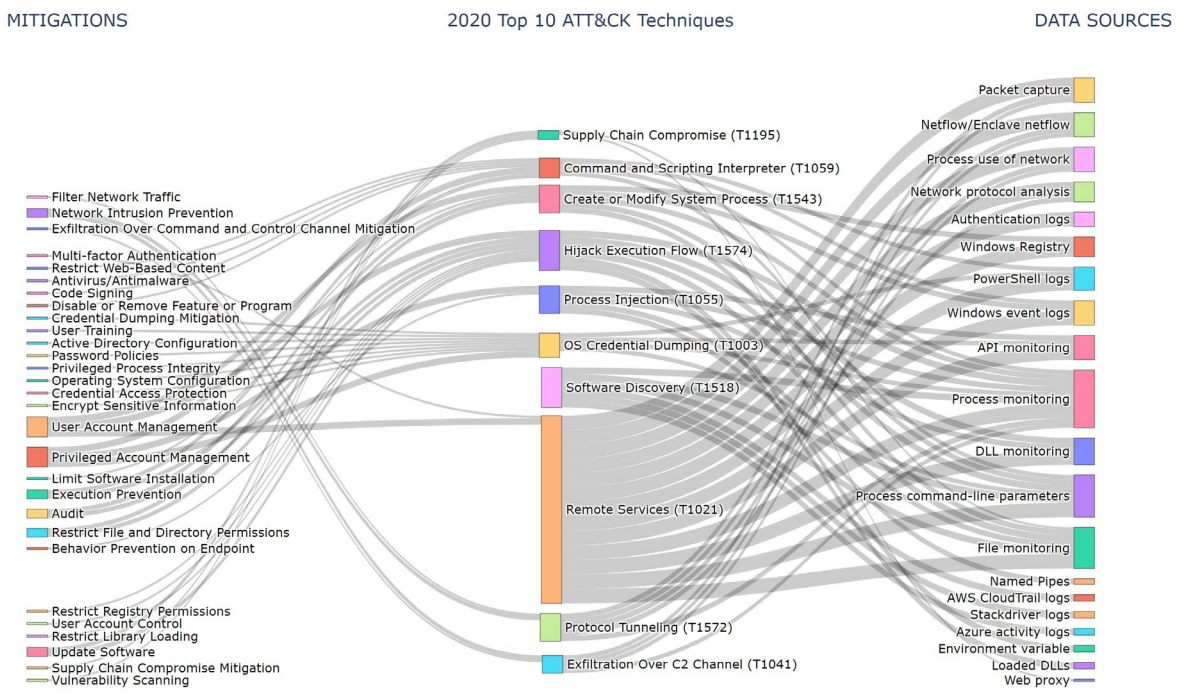
PART 05

全球高级
持续性威胁 APT
研究报告

2020年攻击技战术总结

01.十大ATT&CK核心技战术

MITRE ATT&CK框架[50]是广受业界认可的网络安全攻防战术和技术知识库，提供了可以描述攻击者行为的通用语言，以及针对这些攻击行为的缓解和检测方法。我们根据2020年业界所披露APT报告中的热点技术和360内部海量沙箱检测结果的数据，结合ATT&CK框架提炼了全球APT组织在2020年攻防对抗中所涉及的十大核心技战术攻防知识图谱。



2020年十大核心技战术攻防知识图谱

在2020年十大核心攻击技术的使用趋势中，供应链攻击无疑是今年最为热门的攻击技术，流行的无文件攻击仍然频繁使用恶意脚本、DLL劫持和进程注入等技术，APT组织在攻陷目标后大都提取系统的管理员凭证进一步扩大战果，后门程序越来越着重探测安全软件后再实施不同的对抗策略，内网的横向移动攻击仍以攻击远程Windows服务为主，木马程序越发擅长使用不易被检测的正规加密协议进行通信和盗取数据。除了关注攻击技术，我们在知识图谱中标注了2020十大攻击技术对应在ATT&CK框架中的20种检测数据源和29个预防缓解措施，在知识图谱中这十大攻击技术与左侧的缓解策略、右侧的数据源都保持着紧密的对应关系，这些攻击行为需要对应不同维度的安全数据源才能被发现检测，同时要实施对应的安全策略才能有效缓解防御，对于2020年十大核心攻击技术的检测和缓解有一定的指导意义。

02.利用0day漏洞攻击持续活跃

基于Google Project Zero统计[51]，今年在野0day攻击与去年基本持平。基于浏览器漏洞的攻击占很大比例，今年年初360首次捕获Darkhotel（APT-C-06）使用双星0day浏览器漏洞对中国政府机构进行攻击。另外卡巴斯基披露了PowerFall行动和NSA披露了落鹰行动中VMware Workspace One的0day利用。其他在野0day攻击暂未有安全厂商或机构公开披露APT攻击活动细节。具体0day集合请参看下页列表。

较其他攻击技战术，0day攻击本身成本非常高，常常用于针对高价值目标的定向攻击。由于近几年基于供应链攻击其隐蔽性、攻击成本低且高收益等诸多优势不断体现，很多APT组织在使用0day攻击时会更加谨慎保守，我们预测未来此类0day攻击不会爆发，整体会趋于平稳。

针对移动平台今年年初趋势科技披露[52]，在Google Play商店中发现了响尾蛇组织使用的3个恶意应用程序，它们可以协同工作以破坏受害者的设备并收集用户信息。其中一个名为Camero的应用利用了CVE-2019-2215，该漏洞存在于Binder中，这是在野外首次利用所述UAF漏洞的实例。12月，公民实验室披露[53]NSO Group使用IOS中的iMessage APP中一个无需用户交互的0day漏洞Kismet，该漏洞影响iOS 14之前的版本。在2020年7月和2020年8月期间，至少有36名半岛电视台的记者、制片人、主持人和高管以及在伦敦的一名记者遭攻击。

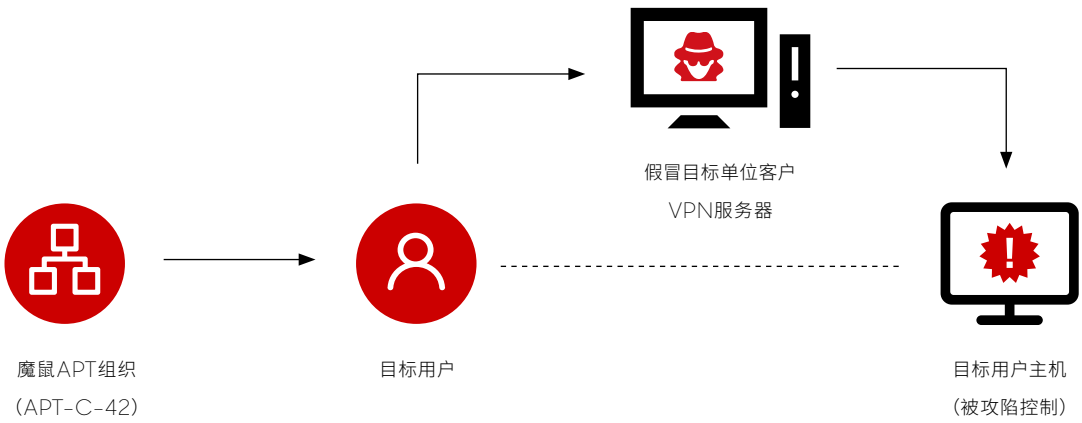
CVE编号	涉及产品	披露厂商
CVE-2019-17026/CVE-2020-0674	IE浏览器和火狐浏览器	360
CVE-2020-6418	Chrome浏览器	Google
CVE-2020-8467/CVE-2020-8468	趋势科技Apex One和OfficeScan XG	趋势科技
CVE-2020-6819/CVE-2020-6820	火狐浏览器	JMPSec
CVE-2020-1020/CVE-2020-0938	微软字体解析远程代码执行漏洞	微软/Google/奇安信
CVE-2020-1027	Windows提权	Google
CVE-2020-1380/CVE-2020-0986	IE浏览器和Windows提权	卡巴斯基
CVE-2020-15999/CVE-2020-17087	Chrome配合Windows提权	Google
CVE-2020-16009/CVE-2020-16010	Chrome浏览器	Google
CVE-2020-27930/CVE-2020-27950/CVE-2020-27932	iOS	Google
CVE-2020-16013/CVE-2020-16017	Chrome浏览器	Google
CVE-2020-4006	VMware Workspace One	NSA

03.疫情影响下VPN成为边界突破新入口

疫情影响下全球化的远程办公让攻击者更好的有的放矢，鱼叉邮件攻击由此达到事半功倍的效果。年初海莲花组织针对我国医疗机构的攻击活动中，对相关目标的大量邮箱发送了含有图片探针的探测邮件，用以探测攻击目标的邮箱是否真实存在。7月蔓灵花发起了“季风行动”更是大规模的邮件钓鱼窃密攻击活动。

在这场全球性疫情博弈之战中，VPN在企业、政府机构的远程办公中起着不可或缺的重要作用，云办公模式也正在经历着繁荣攀升期。但随着疫情的蔓延，不少安全专家也提出了对VPN安全性的担忧，VPN一旦被黑客组织攻陷，众多企事业单位的内部资产将暴露在公网之下，没有任何安全保障，损失将不可估量。

今年鱼叉邮件钓鱼依然是主要的初始攻击方式，但针对VPN、邮件服务器、OA办公系统等远程办公基础设施的攻击也愈发频繁，Fox Kitten组织从2019年至2020年通过多个VPN和网络设备的漏洞入侵企业网络。

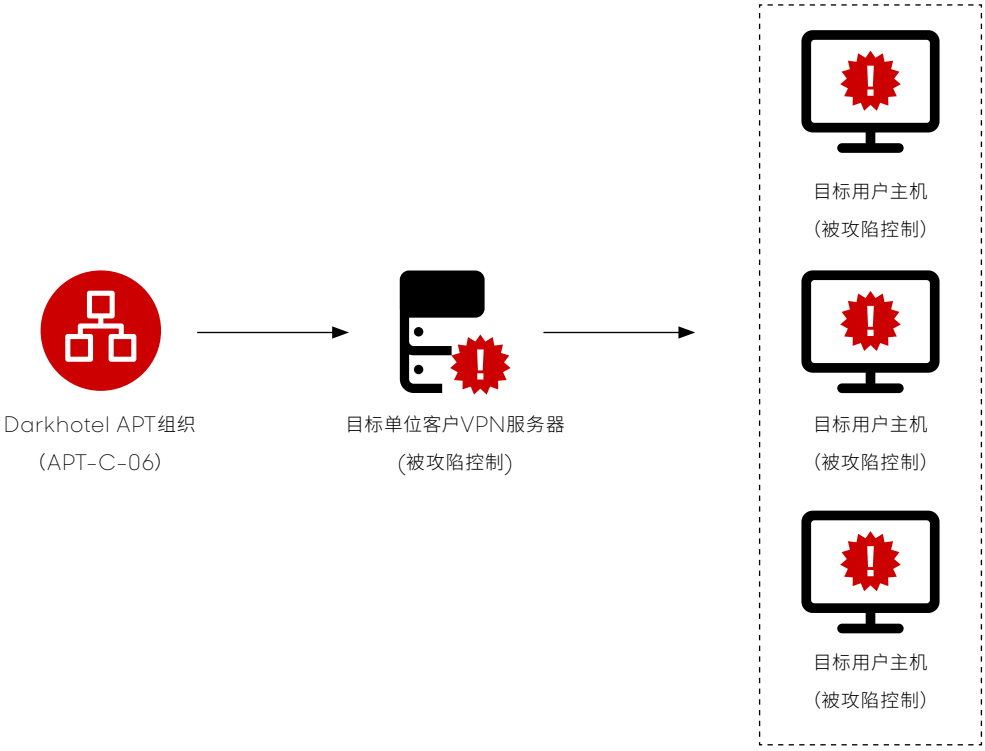


魔鼠APT组织在针对国内某重点供应商的攻击，首先架设了恶意的VPN服务器，进一步通过社会工程学的方式诱导目标用户登录。当目标用户使用存在漏洞的VPN客户端连接恶意VPN服务器时，将自动下载恶意的更新包并执行。

魔鼠组织攻击流程

04.控制基础网络设施

如上章节所述，远程办公基础设施的攻击愈发频繁，VPN、OA系统等，都是都是企业信息化不可或缺的部分。我们4月披露的Darkhotel组织不仅利用了VPN 0day漏洞，还利用了国内某厂商OA系统漏洞进行内网入侵。值得注意的是同期GlobeImposter勒索软件也是利用了国内某厂商OA系统漏洞，使得某行业多个企业受影响。基于控制企业基础网络设施来实现进一步渗透入侵，并不是一种新的攻击手法，但是由于突然性的大规模远程办公将这一场景面临的问题风险不断放大。



Darkhotel利用控制基础网络设施，利用某厂商VPN漏洞攻击流程，利用OA漏洞流程也是类似。

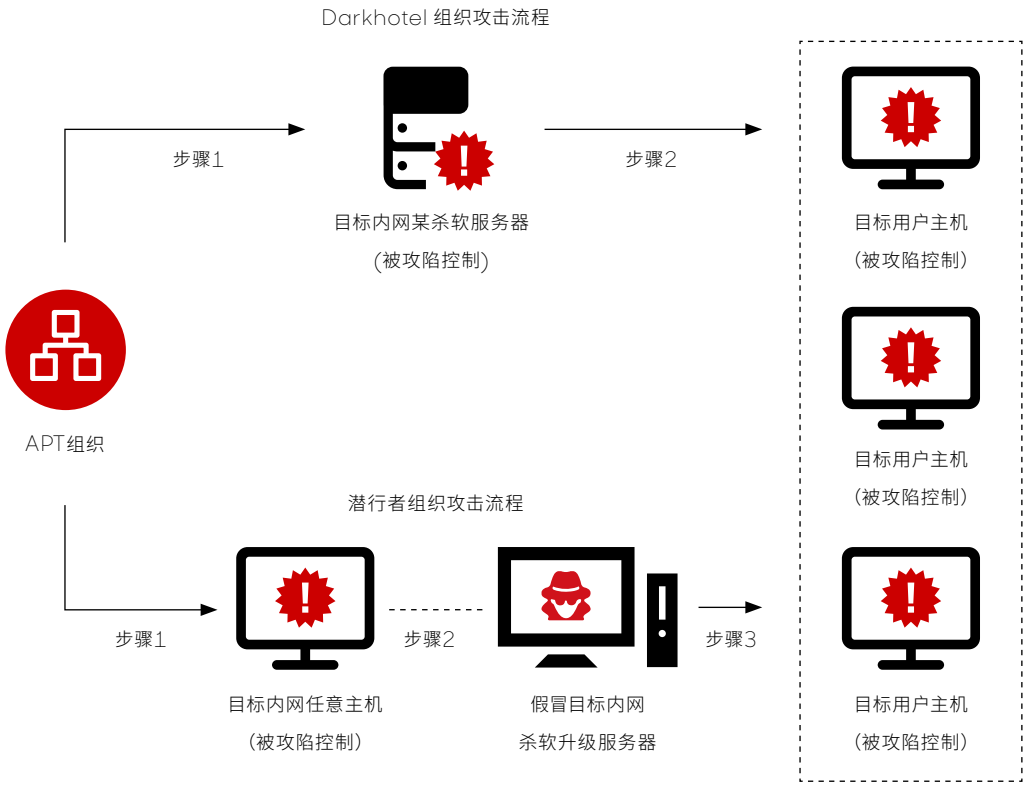
步骤1：攻击者入侵目标单位VPN服务器，并将服务器上关键升级程序替换为木马后门程序；

步骤2：当用户在使用VPN客户端连接服务器时，客户端默认会触发升级行为，导致下载并执行了被替换为后门的恶意程序。另外整个升级过程存在安全漏洞（漏洞编号SRC-2020-281），客户端仅对更新程序做了简单的版本对比，没有做任何的安全检查。导致黑客攻破VPN服务器后篡改升级配置文件并替换升级程序，利用此漏洞针对VPN用户定向散播后门程序。

Darkhotel组织攻击流程

05.安全软件已成为横向移动主要媒介

APT攻击中针对安全防护软件不仅检测躲避进行对抗，现在更多是利用内网安全软件达成下一步目标：横向移动。今年捕获的海莲花、Darkhotel、魔鼠等组织都已将这种方式作为首选，以及历史上其他几个技战术属于头部的APT组织，都曾利用过目标环境内的安防软件进行横向移动。各大APT组织都如此青睐这种攻击方式，主要由于安全类产品内网覆盖高、本身权限较高（节省提权环节）、突破传统隔离阻断等特性。



典型攻击流程1：Darkhotel组织首先攻陷目标内网杀软升级服务器，进一步将更新程序替换为恶意攻击组件，由于杀软客户端更新过程缺乏安全校验机制或被绕过，导致目标内网机器轻松被攻陷。

典型攻击流程2：潜行者组织首先攻击目标内网任意主机，进一步将其构造搭建为某虚假杀软升级服务器，利用杀软客户端漏洞替换升级服务器内网地址，并触发客户端升级操作，导致下载恶意更新包并执行。

利用杀软进行横向移动主流攻击流程

06.命令控制技术变化趋势

由于现今网络大环境对于个人隐私安全愈加重视，各组织机构开始大力推行强制流量加密技术，如浏览器强制执行HTTPS加密、利用DNS over TLS (DoT)加密DNS通信等。另一方面攻击者对网络流量安全设备的攻防也开始更加重视，趋于将C2网络通信流量与正常流量混合，以此来隐藏C2通信，以绕过流量安全检测防护为目来进行命令控制。这些技术趋势的变化和攻防技术的演进，都给流量安全检测带来了巨大的挑战。

命令控制 (C&C 或C2) 是在APT攻击阶段中最核心的一环，后门程序通过自定义的C2通道与控制服务器进行通信交互，攻击者对受害者进行控制从而实施真正造成危害的攻击活动。在2020年的APT攻防对抗中，我们看到命令控制技术对抗安全检测的许多变化趋势。

C2构建	以往技战术	今年特点
基础设施	不做任何隐蔽的独立服务器	C2服务器伪装成exchange邮件服务、开源的云存储服务器，或利用第三方的正常云服务作为C2服务器中转
通信协议	使用自定义协议和常规的HTTP[S]协议，对流量不做任何伪装	使用WebSocket协议、伪装成云对象存储请求等，将命令控制隐藏在正常的网络请求和网络应用行为流量内
C2域名	域名解析IP不做任何保护	利用域前置技术将C2域名伪装为正规域名，真正的C2域名和基础设施藏于CDN服务商背后
控制形式	直接粗暴的反向连接	通过DNS隧道向外部服务器报告主机信息，根据信息判断再激活下一阶段的恶意代码

PART 06

全球高级
持续性威胁 APT
研究报告

2021年APT趋势预测

01.针对中国的国家级网络攻击，APT组织数量和攻击活跃程度可能会超过今年

2020年境外APT组织针对我国相关机构或个人的攻击活动异常频繁，较去年持续上升，APT攻击正逐渐呈现出常态化、高频率的特性。由于地缘关系、新冠肺炎疫情的持续影响等长期问题，以及从针对我国活跃组织数量不断的增加趋势推测，我们预测明年已知APT组织依然会持续攻击，而且攻击程度会进一步增加。另外新组织或历史未知攻击会不断浮现出来。尤其在围绕“十四五规划”和2035年远景目标[54]等相关政策方向、新技术研究落地期间，这类多个APT组织都会关注的领域，相关攻击会更活跃，尤其在某些技术有重要突出的时刻可能会出现集中攻击的情况。

02.围绕“新冠肺炎疫情”话题的攻击将持续活跃

2020年初，在新冠疫情给全球格局带来新的冲击影响下，境外APT组织针对我国的攻击活动异常频繁。利用新冠肺炎热点事件进行诱饵定向攻击已成常态主流，目前全球范围内累计新冠肺炎的确诊人数更是已经突破7000万人，对于全球疫情防控形势，张文宏专家也做出分析[55]，他认为至少在未来的1-2年内全球范围的疫情都不会结束。随之而来的APT攻击也会持续围绕，在全球疫情控制过程中重大进展突破或变化，都可能会导致相关攻击的短期突增活跃。

03.涉及远程办公基础设施的攻击将越发频繁

2020年春节后，在新冠肺炎疫情初步得到控制和复工初期，远程办公几乎成为企业和用户唯一的选择，继而相关配套信息化基础设施也必须加速建设。进一步如VPN、邮箱等远程办公基础设施的安全问题也随之而来。3月，全国信息安全标准化技术委员会秘书处针对远程办公安全问题，组织相关厂商和安全专家，编制并发布了《网络安全标准实践指南—远程办公安全防护》[56]。另外今年我们已经捕获到多起利用远程办公的定向攻击活动，如披露的Darkhotel利用VPN漏洞的攻击活动。

全球范围内的疫情不会短期结束，虽然目前中国等部分国家疫情基本得以控制，大部分企业已恢复驻地办公，但由于疫苗大范围接种、病毒变异等诸多变化因素。远程办公方式将一直持续并在一些企业已经转换为主要办公方式，如微软下半年公布的允许员工永久远程办公等。

04.以供应商为核心目标的供应链攻击将常态主流化

2020年针对供应链的攻击已成为APT组织主要使用的技战术之一，而且聚焦针对供应链中供应商进行定向攻击。今年披露的Darkhotel针对VPN的攻击，魔鼠针对某邮件系统供应商的攻击，以及海莲花组织今年针对多个大型IT供应商，相关供应商的客户主要涉及国内教育、通信和政府行业。另外12月披露的针对Solarwinds攻击，堪称史上影响力最大的供应链攻击行动，几乎是核弹级别的供应链攻击。

由于供应商一般没有针对性的防御措施，而且大部分都是提供行业解决方案或定制化服务，即攻陷某一供应商，则所涉及行业相关单位也都在掌控中，这使得一般以行业为目标的APT攻击事半功倍，大大降低了攻击成本。另一方面是由于长期渗透攻击并不是直接针对目标，待对供应商完全可控后，再对最终目标发起攻击，往往这过程中并不会留下过多中间过程等攻击痕迹，这导致发现滞后，整个攻击过程都是以年为单位。

基于以上分析我们认为未来供应链攻击会持续推陈出新，针对目标上游的供应商攻击将会成为APT攻击中的标准打法。

05.继续紧密围绕政治、经济等热点领域及事件，以网络间谍活动为主

2020年我国政府、教育和国防军工是重灾区，其中教育领域更多是针对高校科研课题等，其意图是窃取围绕新兴技术、军事科研等最新机密。具有国家背景的APT组织，政府、军工、科技等领域是长期持续的攻击目标，尤其是地缘政治相关的攻击，将继续成为常态，且由局势的变化会直接影响攻击频次活跃度。涉及医疗行业由于新冠肺炎疫情的长期持续影响，在出现重大突破或进展时会成为短期攻击目标。

随着“新基建” 时代我国信息基础设施快速发展的同时，除了不断尝试针对新领域的攻击探测，APT攻击也将伴随着5G和物联网技术的发展具备更强大的攻击能力，如越来越多的物联网设备将成为APT组织新的战备物资。

在过去几年间，全球各国央行都看到了货币数字化的大趋势，并加大了相关投入，我国政府很早就看到了央行数字货币在推动人民币国际化中的蕴藏的机遇，并积极探索和推进。随之而来的是以国家背景的APT组织，不像以Lazarus组织以牟利为目的，而更多是想偷窥中国在数字货币探索实施的情况和政策战略方针。

另外值得注意的是APT攻击实施过程中会呈现出对相关单位或个人有极强的针对性，但在涉及的目标领域或行业则会尽可能的更全面，如针对军工领域，相应涉及的央企、科研院所、教育机构等都会成为重点攻击目标。

06.未知APT组织将愈发增多，归因需长期持续研判

2020年越来越多的未知APT组织开始涌现，APT组织的归因问题取决于APT攻击活动中可供关联的数字证据是否充足，而安全厂商的安全数据资源是否足够庞大和丰富也决定了攻击归属的难易。由于各个安全厂商安全数据的差异，因此也会导致不同的分析视角，对同一APT组织的归属、归因存在争议，在360看来APT组织的归属是需要进行长期持续研判的。

目前360安全大脑持续监控的APT组织已经超过了50个，但其中仍有多个APT组织未划分归属。以摩诃草组织(APT-C-09)为例，我们在南亚地区APT组织2019年度报告中披露了一款全新的后门程序，以该后门的pdb文件将其命名为了cnc_client，由于该后门程序的攻击活跃时间、攻击目标与摩诃草组织重合，以及部分利用GITHUB下载后门的相似手法，我们将攻击归属于了摩诃草组织(APT-C-09)，认为是该组织使用的众多后门程序之一，而后其他安全厂商也纷纷引用了其归属。但cnc_client后门在后续的攻击活动却让我们归属确认产生了动摇，以CNC小组定义其攻击活动，由于该后门后续的攻击活动展现了完全的独立性，建立了完全独立的C&C和

鱼叉攻击基础设施，利用新冠肺炎疫情等相关题材发动了针对医疗机构的定向攻击，而非摩诃草组织关注的科研、教育和智库领域，也没有和摩诃草组织(APT-C-09)历史攻击数据发生明显关联，所以其后续的攻击活动应该确定为未知APT组织的攻击活动。

另一个例子是魔鼠(APT-C-42)，该组织最早的攻击活动在2017年，其在2018年日本互联网应急响应中心认定为僵尸网络，但在今年美国因为其针对疫苗开发机构的攻击将其归属为APT29组织，而360安全大脑在2019年8月-2019年9月期间就观测到了该组织针对我国的供应链攻击行动。这个组织的攻击活动被认定为是APT攻击整整跨越了3年时间，同时该组织的网络武器和技战术完全是有自身鲜明特点，与APT29组织的技战术没有明显关联，同时历史上也未曾披露APT29组织针对我国的攻击行动，因此我们有理由认为这也是一个全新的未知APT组织。

07.意图为破坏、窃密的针对性勒索攻击将不断出现

2020年针对性定向勒索攻击大幅上升，针对英特尔、富士康、巴西航空工业公司、日本汽车制造商本田等大型企业的勒索攻击就有二十多起。其中今年3月Visser Precision制造商遭受勒索攻击[57]，并被攻击者将窃取的机密文件公之于众，导致其重要客户受到影响，如：特斯拉、波音、洛克希德·马丁公司和SpaceX等行业巨头公司。这些被勒索的企业都造成了不同程度的机密数据泄露、业务中断等重大影响。

由此可见这些以牟利为主的勒索攻击，其危害影响似乎不亚于一场APT攻击，它能爆发的威力似乎比我们想象的还要严重。那勒索攻击是否仅定性为金融犯罪，其攻击意图只为获得赎金？2017年，利用伪装成NotPetya的勒索病毒发动了针对乌克兰政府、金融和能源机构的攻击[58]；今年卡巴斯基披露的由Lazarus组织运营的VHD勒索软件[59]；疑似背后是伊朗政府的勒索软件组织Pay2Key，12月20日声称攻陷了以色列最大的国防承包商——以色列航空航天工业公司（IAI）[60]，在此之前该组织已经攻击了多家以色列公司。以及我们发现针对国内某行业的勒索攻击中，即使用户愿意尝试支付赎金，但也没有任何有效信息可以联系到攻击者。

针对这些攻击我们很难确定攻击者实际目的，但确定的是攻击给用户造成了严重的影响。勒索攻击和APT攻击之间的交集逐渐增多，勒索攻击更像是一场精心策划的APT攻击中的烟雾弹，将其真实攻击意图掩盖。

PART 07

全球高级
持续性威胁 APT
研究报告

附录

01

360安全大脑

360基于安全大数据、知识库和专家，建设了360网络安全大脑和网络安全基础设施（情报、漏洞、专家、实战、培训、测绘、开发），以云服务方式为政府、企业、个人用户提供安全公共服务，形成了新的安全理念和方法论。

360网络安全大脑强化了“精准防控为要、实战有效为王”的价值取向，着眼安全事件的“高效发现和及时处置”，理顺识别、防御、监测、预警、响应流程，推动一般常见风险及时处置、高级重大威胁有效解决、预防关口主动前移。着眼防范化解重大风险，聚焦最难啃的骨头、最突出的隐患、最明显的短板，及时总结网络安全风险防控经验，研究开发务实有效的安全原生服务。强化互联网体系与政企体系的协同联动，让网络安全体系回归保障业务的本质。

02

研究机构

•360高级威胁研究院

360高级威胁研究院是360政企安全集团的核心能力支持部门，由360资深安全专家组成，专注于高级威胁的发现、防御、处置和研究，曾在全球范围内率先捕获双杀、双星、噩梦公式等多起业界知名的0day在野攻击，独家披露多个国家级APT组织的高级行动，赢得业内外的广泛认可，为360保障国家网络安全提供有力支撑。

•360烽火实验室

360烽火实验室致力于移动恶意软件分析、移动灰黑产研究、移动威胁预警、移动APT的发现与追踪等移动安全领域的深入研究。作为全球顶级移动安全生态研究实验室，360烽火实验室在全球范围内不仅首发了多篇具备国际影响力的移动安全生态研究成果，并且成功狩猎了蔓灵花、拍拍熊、北非狐等多个APT组织针对我国及境外重要目标的攻击活动。实验室在为360手机卫士、360手机助手、360加固保等公司产品提供核心安全数据的同时，也为科研单位、手机厂商、应用商店及上百家国内外合作伙伴提供了移动应用安全检测服务，全方位守护移动安全。

•360网络安全研究院

360Netlab（网络安全研究院）是360公司负责大网范围内的基础网络数据安全分析和僵尸网络发现、分析和跟踪的核心研究部门。其运营着国内公开的最大和最悠久的PassiveDNS数据库，其研发的DNSMon系统在无规则的情况下，提前发现并拦截了数十种恶意程序所使用的主控域名。在僵尸网络研究方面，首次发现并命名了如satori，godlua，DDG，Gpon，Mozi等十余种众多影响巨大的僵尸网络。同时积极参与国际合作共同打击网络犯罪，获得了美国司法部和FBI的多次公开致谢。

•360反病毒部

360反病毒部是360政企安全集团的核心能力支持部门，由360一线对抗防御专家组成，负责流行病毒木马的监测、防御、处置和新安全威胁研究。维护有360主防系统、360反勒索服务等基础安全服务，为用户提供有横向渗透防护、无文件攻击防护、软件劫持防护、挖矿木马防护等多项防护功能，近年来发布有WannaRen勒索病毒调查，外贸企业钓鱼攻击分析等各类安全风险提醒，保护广大网民上网安全。

参考链接

1.https://mp.weixin.qq.com/s/lh7y_KHUxag_-pcFBC7d0Q

2.https://mp.weixin.qq.com/s/KsEyD0HpKMcuZbBcYADpAA

3.https://blogs.360.cn/post/apt-c-06_0day.html

4.https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/

5.https://mp.weixin.qq.com/s/zV0FL1MZVvGW-FNY9wDbOg

6.https://mp.weixin.qq.com/s/h_MUJfa3QGM9SqT_kzcdHQ

7.https://i.blackhat.com/USA-19/Wednesday/us-19-Burke-ClickOnce-And-Youre-In-When-Appref-Ms-Abuse-Is-Operating-As-Intended.pdf

8.https://mp.weixin.qq.com/s/5No0TR4ECVPp_Xv4joXEBg

9.https://b.360.cn/about/news/article5f15869528566f0055ff2524

10.https://blogs.jpcert.or.jp/en/2018/07/malware-wellmes-9b78.html

11.https://www.solarwinds.com/securityadvisory

12.https://www.welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal/

13.https://www.fireeye.com/blog/threat-research/2019/04/spear-phishing-campaign-targets-ukraine-government.html

14.https://www.trendmicro.com/en_us/research/20/a/first-active-attack-exploiting-cve-2019-2215-found-on-google-play-linked-to-sidewinder-apt-group.html

15.https://securelist.com/transparent-tribe-part-1/98127/

16.https://www.clearskysec.com/wp-content/uploads/2020/08/Dream-Job-Campaign.pdf

17.https://www.crowdstrike.com/blog/who-is-pioneer-kitten/

18.https://www.forbes.com/sites/zakdoffman/2020/02/16/terrorist-android-malware-exposed-here-are-the-hamas-apps-that-targeted-israeli-soldiers/?sh=6b07321223ae

19.https://blogs.360.cn/post/apt-c-23_target_at_middle_east.html

20.Hiding in plain sight: PhantomLance walks into a market | Securelist

21.https://blogs.360.cn/post/apt-c-50.html

22.https://b.360.cn/about/news/article5f6ff23e46a3f50057643944

23.https://mp.weixin.qq.com/s/gWOIRNPLVqX761LW8x-S5g

24.https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

25.https://www.bbc.com/russian/features-49050982

26.https://www.anquanke.com/vul/id/2049794

27.https://www.cert.org.cn/publish/main/12/2015/20150914152821158428128/20150914152821158428128_.html

28.https://www.anquanke.com/post/id/86657

29.https://securelist.com/operation-shadowhammer/89992/

30.https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198b

31.https://mp.weixin.qq.com/s/KS9iw8EosGVI_1Lhsq2g3w

32.https://sindh.gov.pk/NOTIFICATIONS/January2020/Advisory23-1-20.pdf

33.https://kashmirexclusive.in/2020/05/01/intel-agencies-caution-armed-forces-against-pak-propped-fake-aarogya-setu-mobile-app/

34.https://securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf

35.https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html

36.https://m.threatbook.cn/detail/2371

37.https://blog.alyac.co.kr/2896

38.https://securelist.com/deathstalker-mercenary-triumvirate/98177/

39.https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/

40.https://www.recordedfuture.com/pupyrat-malware-analysis/

41.https://blog.talosintelligence.com/2020/04/poetrat-covid-19-lures.html

42.https://www.zscaler.com/blogs/security-research/targeted-attacks-oil-and-gas-supply-chain-industries-middle-east

43.https://www.securityweek.com/ransomware-operators-demand-14-million-power-company

44.https://www.businessinsider.in/tech/news/mumbais-massive-power-cut-last-month-may-have-been-the-work-of-hackers/articleshow/79318282.cms

45.https://cryptome.org/2014/12/nsa-aurora-gold-intercept-14-1203.pdf

46.https://mp.weixin.qq.com/s/NN_iRvwA6yOHFS9Z3A0RBA

47.https://www.telsy.com/wp-content/uploads/DeadlyKiss_TAAR.pdf

48.https://securityaffairs.co/wordpress/101134/security/rostelecom-telco-hijacks-internet-traffic.html

49.https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

50.https://attack.mitre.org/

51.https://docs.google.com/spreadsheets/d/1IkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/view#gid=1869060786

52.https://www.trendmicro.com/en_us/research/20/a/first-active-attack-exploiting-cve-2019-2215-found-on-google-play-linked-to-sidewinder-apt-group.html

53.https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/

54.http://www.xinhuanet.com/politics/2020-11/03/c_1126693293.htm

55.https://weibo.com/7454177482/Jxq2v8Ay5?type=comment

56.https://www.tc260.org.cn/front/postDetail.html?id=20200313141548

57.https://mp.weixin.qq.com/s/WvLHs6lulOSeYUgVE8JTkg

58.https://www.reuters.com/article/us-ukraine-cyber-attacks-idUSKBN19I1IJ

59.https://securelist.com/lazarus-on-the-hunt-for-big-game/97757/

60.https://www.timesofisrael.com/iran-linked-group-claims-to-hack-israeli-defense-firm-releases-employee-data/

2020

全球高级持续性威胁

APT

研究报告

360政企安全 360 高级威胁研究院