360政企安全 | 360 高级威胁研究院

2021/上半年

全球高级持续性威胁

APT

研究报告

RESEARCH REPORT

- 攻击概览
- 2021上半年活跃组织
- 2021上半年攻击态势总结
- 关键核心战场态势

2021/上半年

全球高级持续性威胁 APT 研究报告

CONTENTS

CONTENTS

04

关键核心战场态势

05

PART 01

2021上半年攻击概览

2021年上半年，全球高级持续性威胁（APT）整体形势依然严峻，发现和披露的APT攻击活动较去年同期大幅增加。上半年全球公开报告数量492篇，其中披露的攻击活动涉及APT组织90个，首次披露的组织17个，无论报告数量还是组织数量都已超去年同期。从全球范围看，APT攻击活动还是重点关注政治、经济等时事热点。目标主要针对政府、国防军工、科研等行业领域。今年全球疫情仍然肆虐，局部地区疫情形势相比去年甚至更加严峻，围绕“新冠疫情”开展的相关攻击活动继续处于高位。上半年攻击活动中利用的0day漏洞数量已超过去年全年总和，达到历史新高。上半年爆发的针对美国最大燃油管道运营商和爱尔兰卫生服务部门在内的一系列针对关键基础设施的勒索攻击事件，体现出勒索攻击不断APT化的发展趋势。勒索威胁逐渐上升到事关国家安全的层面，已成为全球网络安全的共同挑战。

今年上半年，我国率先进入疫情后全面经济复苏和建设阶段，在此新形势下，境外APT组织针对我国的攻击持续活跃，较去年同期大幅上升。依托强大的安全能力，360在过去累计发现了46个其他国家背景的APT组织，监测到3600多次对中国的国家级网络攻击。上半年，360捕获到对中国地区发起攻击涉及的组织12个，其中首次发现的组织2个：芜琼洞、伪猎者。针对中国地区的APT攻击事件统计结果显示：境外APT组织依然针对我国政府、科研和国防军工等领域重点目标，其中来自于东亚、南亚和东南亚的APT组织针对我国攻击最为活跃。对向教育领域高等学校的攻击活动进行分析发现，攻击瞄准的目标实则是我国国防军工和科技创新体系，反映出APT组织通过对关键行业横向领域的攻击和渗透，从而进一步实现对目标行业的攻击。在南亚、东南亚地区疫情反弹期间，针对医疗卫生、媒体行业的攻击凸显。另外，针对城市区域性的攻击威胁持续不断，加以万物互联下，智慧城市的攻击面不断扩大，城市数字化转型下APT威胁加剧。ICT供应链攻击威胁进一步升级，针对中介招标代理机构的攻击愈发频繁。

今年是“十四五”开局之年，我国将开启全面建设社会主义现代化国家新征程、向第二个百年奋斗目标进军，随着数字经济进入新的发展阶段，我国网络安全建设面临着新的挑战和不稳定因素。此次疫情加速了全球政治经济格局重塑，未来在后疫情时代，全球经济逐步进入复苏阶段。在地缘政治、治理体系潜在风险等因素的影响下，加之世界经济重心东移趋势日显，势必会导致大国博弈更加激烈。在此新形势下，针对我国的国家级网络攻击，APT组织的数量和活跃程度以及攻击技战术的复杂度，或将超过以往。国家级的高级威胁防御领域更加需要包含360政企安全在内的广大网络安全企业和从业者同心协力，为国家各项基础设施建设保驾护航，守卫社会主义现代化建设成果，为坚定不移建设制造强国、质量强国、网络强国、数字中国贡献力量。

PART 02

2021上半年活跃组织

360高级威胁研究分析中心监控发现，2021年上半年全球活跃的APT组织有90个，其中有17个是首次披露。针对我国攻击活跃的APT组织有12个，其中新发现暂未被其他厂商披露的APT组织有两个：APT-C-59（芜琼洞）、APT-C-60（伪猎者）。毒云藤、蔓灵花和海莲花这三个组织针对我国的攻击活动最为活跃，长期持续攻击我国多个行业领域重点目标。Darkhotel、响尾蛇组织相比去年攻击频次有所减弱，但呈现阶段性集中攻击后快速隐匿现象。另外比如CNC、新组织芜琼洞短期集中攻击特性更为明显，尤其在其关注的热点事件先后活动最为频繁。

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组织进行综合评估，得出APT组织的攻击活跃度排名。

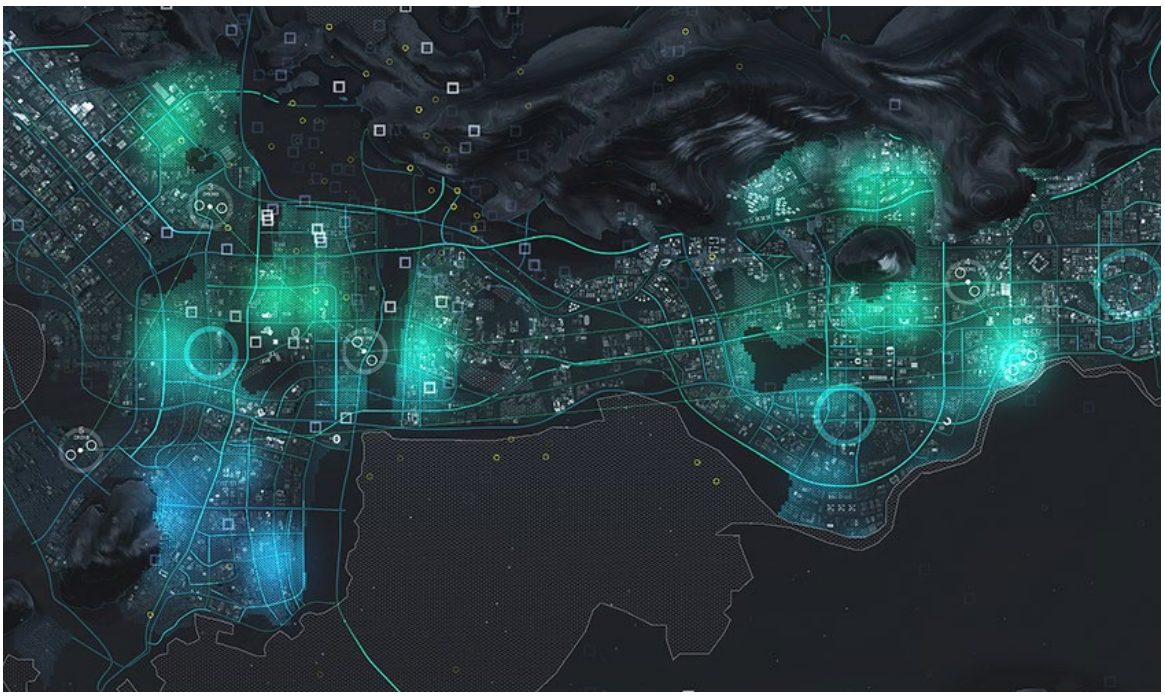
排名	组织名称	涉及行业
TOP1	APT-C-01（毒云藤）	政府、教育、科研等
TOP2	APT-C-08（蔓灵花）	教育、军工、科研等
TOP3	APT-C-00（海莲花）	ICT供应商、政府、教育等
TOP4	APT-C-06（Darkhotel）	贸易、科研、媒体等
TOP5	APT-C-59（芜琼洞）	媒体、科研、医疗等
TOP6	APT-C-48（CNC）	教育、科研
TOP7	APT-C-55（Kimsuky）	政府
TOP8	APT-C-60（伪猎者）	贸易、政府
TOP9	APT-C-24（响尾蛇）	政府、医疗、建筑
TOP10	APT-C-47（旺刺）	贸易、制造、建筑

• 2021年上半年针对中国地区TOP10境外APT组织

1.南亚

南亚地区APT组织常年活跃，针对我国和其他南亚地区国家，主要围绕地缘政治相关。从去年下半年开始南亚APT组织攻击活动不断活跃，相关上升趋势一直持续至2021年5月初，尤其今年第一季度相关攻击较去年大幅增加，主要涉及教育、政府和国防军工多个领域。而从5月之后攻击有所减缓，但陆续出现多起针对我国医疗卫生机构的攻击活动，我们推测近期攻击活动减缓和针对医疗行业更具针对性，可能是由于4月份，南亚地区疫情再次爆发有关。

今年上半年蔓灵花组织针对我国的攻击活动最为活跃，相比之下响尾蛇、CNC攻击频次较低但更具针对性。除蔓灵花以外，肚脑虫、透明部落、幼象等其他组织主要针对巴基斯坦、印度等南亚国家。



01.APT-C-08 (蔓灵花)

从去年9月份开始出现的chm文档攻击方式中，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,此类攻击方式在今年更加主流。除鱼叉邮件附件投递之外，更多还是仿冒目标单位邮箱系统的钓鱼网站攻击，其占比达到7成。去年年底蔓灵花组织积极探索的一种新型供应链攻击，今年已成常态主流。这类攻击目标并不是供应商和最终目标需求方，而是针对起到中介服务的招标代理机构。

在锁定重点目标后，蔓灵花组织进一步会不惜采用0day漏洞进行渗透攻击。今年上半年披露的0day漏洞攻击已有两起，今年2月，国内安全厂商安恒信息年初披露了该组织2020年12月的攻击活动中[1]，使用了WINDOWS内核提权0day漏洞 (CVE-2021-1732) 。

另外在广泛使用的仿冒目标邮箱系统的钓鱼攻击中，蔓灵花除了克隆目标邮件系统以外，还会使用某一文档文件作为背景。当登录成功后则跳转至该文档文件的页面，使得钓鱼网站更加难以辨别。

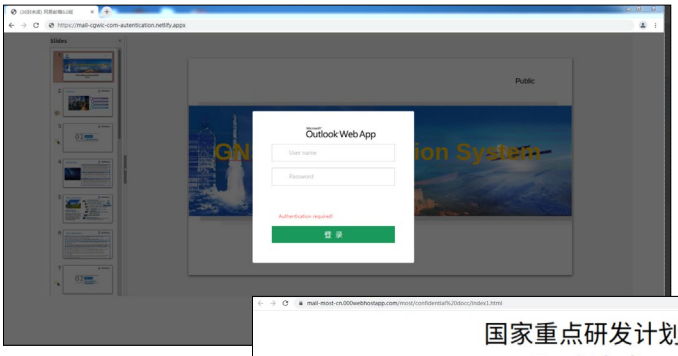


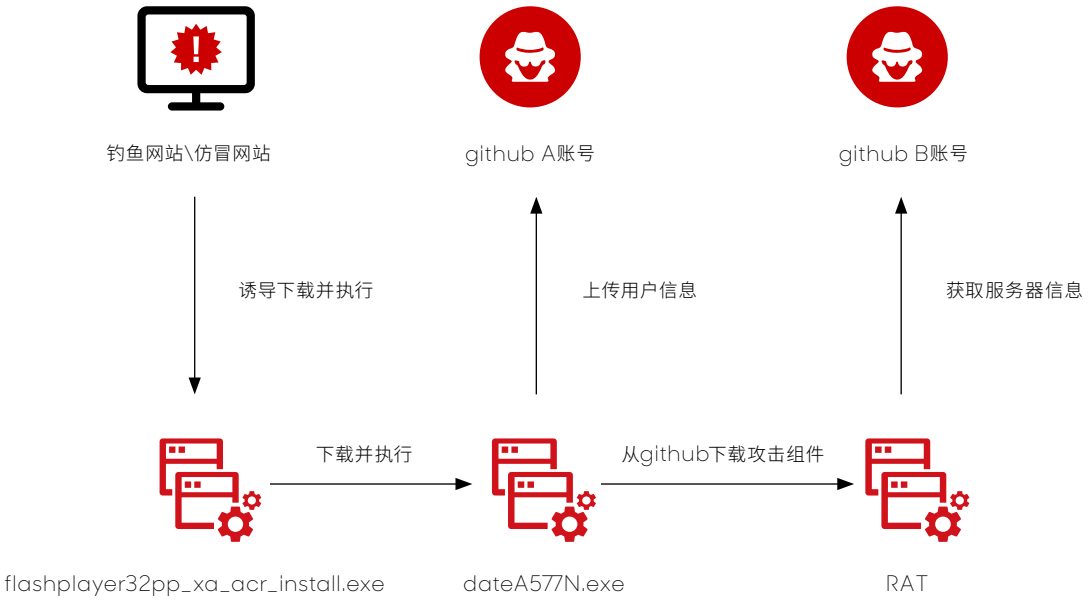
图1

图2

• 图1.蔓灵花-诱饵文档作为背景实例1 • 图2.蔓灵花-诱饵文档作为背景实例2

02.APT-C-48 (CNC)

2021年4月，我们捕获到CNC组织针对我国重点单位发起了新一轮的攻击[2]。该组织上次攻击行动还是在去年年初国内疫情爆发期间，针对我国医疗行业发起集中攻击。值得注意的是，蛰伏许久的CNC组织，在今年6月中旬我国航天时事热点前后，针对我国航空航天领域相关的重点单位突然发起集中攻击。



CNC组织今年最新的GithubJoint攻击流程如图所示，整个攻击过程中利用多个github账户来完成样本下发、C&C更新、用户信息记录等功能。另外相关GitHub账号是在4月份投放到实际攻击活动中，但是早在1、2月份已进行多次测试。

• GithubJoint攻击流程

最终驻留的恶意程序是基于GRAT2开源远控，进行大量修改后的定制化版本。其中CNC小组对部分指令编码进行了修改。使用了多个国家的语言来进行替换，推测CNC组织成员有可能是想在规避GRAT2的指令特征的同时，混淆安全分析人员对CNC组织幕后所属国家的判断。其中两者部分指令对比如下:

程序内指令	使用语言	对应翻译	GRAT2原指令	功能
herunterladen	德语	download	download	上传指定路径文件的数据到服务器
hosutomei	日语	hostname	hostname	获取设备计算机名
hochladen	德语	upload	upload	下载文件到指定路径
sortie	法语	exit	exit	退出程序
ekranokopija	立陶宛文	screenshot	screenshot	上传屏幕截图
chisono	意大利语	who I am	whoami	获取设备用户名
fearann	爱尔兰语	domain	domain	获取设备域FQDN
elenco	意大利语	list	ps	遍历获取当前进程信息

• CNC恶意组件部分指令

03.APT-C-35（肚脑虫）

肚脑虫组织今年上半年依然主要针对巴基斯坦政府、国防军工的重点目标发起攻击。今年6月我们披露了该组织最新的后门框架[3]，根据这些后门框架使用的组件名，将其命名为“Jaca“框架。在该框架中通过Downloader与服务器交互下载并调用其他组件。并且由于驻留样本隐蔽性极强，我们发现往往肚脑虫对攻击成功的设备存在较强的控制力。

相比往年该组织使用的后门框架，这套框架采用了函数动态导入+函数名加密的方式来隐藏调用的API函数，并对多数使用到的字符串和数据进行加密，暴露的信息更少。而后的框架版本更是在路径和文件名上采用了更加贴合windows系统的命名，在欺骗性上得到极大的提升。

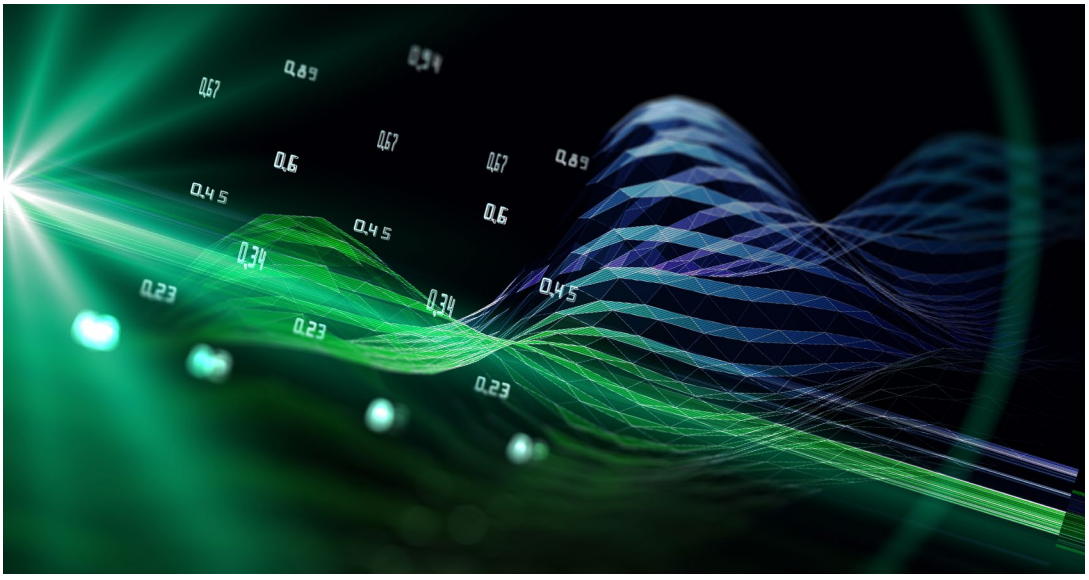
2021.6-至今	2020.11-2021.5	2019.12-2020.10	YTY框架	功能简述
igfcServicee.dll	JacaPM.dll	NumberAlgo.dll	Boothelp.exe	下载组件 并执行
winlogup.dll	JacaUL.dll	COMEvent.dll	abode.exe	功能组件 相关文件上传
winlogss.dll	JacaSP.dll	ScnPoint.dll	dspcheck.exe	截图工具
winlogdfl.dll	JacaDFIter.dll	Dormode.dll	vstservice.exe	文件搜集
winlogkl.dll	JacaKL.dll	FrameCordi.dll	mdriver.exe	键盘、鼠标 消息记录
winlogbw.dll	JacaBD.dll	SRCPolicy.dll		浏览器 敏感信息窃取
winlogus.dll	JacaUSD.dll			移动磁盘 文件搜集

• 肚脑虫历年使用的后门框架汇总

04.其他

APT-C-24（响尾蛇），今年的攻击活跃程度较去年有一定幅度的减弱，相关攻击活动中依然延续了去年的攻击手法，通过鱼叉邮件投递lnk快捷方式或带有公式编辑器漏洞的rtf文档文件来完成攻击活动。但攻击者反侦察意识逐步提高，攻击隐蔽性有明显加强，从C2有效时长、URL格式变化、HTA组件替换为.net模块反射加载等都有所变化，其中比如响尾蛇组织开放的下载链接有效时长，已经缩短至几小时甚至几十分钟，这在一定程度上加大了安全研判人员的进一步追踪溯源的难度。

APT-C-56（透明部落），长期针对周边国家和地区，主要是印度、阿富汗等相关政府、军事进行定向攻击活动。今年该组织攻击活动持续活跃，4月，我们披露了该组织利用新冠疫苗疫情热点事件针对印度医疗行业的定向攻击活动[4]，6月，我们披露了该组织针对印度军事相关目标的攻击活动[5]，本次攻击活动使用了一种新的Android恶意软件，根据恶意软件包结构我们将其命名为PJobRAT，PJobRAT主要伪装成印度婚恋交友和即时通讯软件。通过对同源样本进行分析，我们推测本次攻击时间从2021年1月开始，3月至5月攻击最为频繁。



2.东亚

今年上半年东亚地区众多APT组织，针对我国的攻击活动最为频繁，其中以毒云藤为首，长期大量使用钓鱼邮件攻击我国多个行业领域重点单位，而Darkhotel、芜琼洞和伪猎者攻击活动并未像毒云藤那样频繁，但攻击更具集中针对性。芜琼洞和伪猎者这两个组织是我们今年首次发现，基于相关技战术和武器资源我们初步判定是源于朝鲜半岛地区。

Lazarus组织上半年的攻击活动依然积极活跃，尤其是利用社交媒体针对安全研究人员的攻击。Kimsuky、Scarcruft上半年的攻击也非常活跃，主要围绕朝韩关系、新冠疫情、核问题等针对政府、媒体等目标。

01.APT-C-01 (毒云藤)

毒云藤组织今年上半年的攻击异常活跃，较去年明显上升，是针对我国攻击活动最为频繁的组织。该组织长期针对国内政府、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，且攻击活动范围基本仅限于我国，其最早的攻击活动可以追溯到2007年。上半年的攻击活动中，该组织持续制造大量假冒国内知名邮箱服务网站，以及假冒受害目标单位邮箱系统网站，围绕时事热点针对政府机构、国防军工、科研等多个领域的重点单位发起钓鱼邮件攻击。

毒云藤组织经常利用各类时事热点发起攻击，典型事件如：1月基于交通整治类热点事件攻击国内多个交通监管机构；4月多个单位展开实网攻防演练，毒云藤组织则依托演练诱饵关键词针对某智库发起定向攻击；5月又以个税申报活动、五一疫情防控等热点事件针对多个行业和机构发起定向攻击。

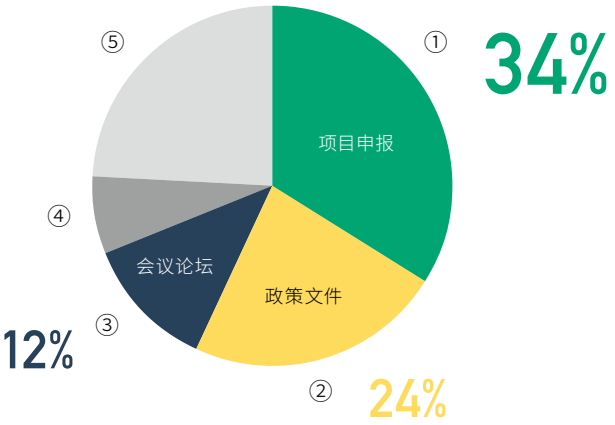
图1

图2

- 图1.毒云藤-利用实网攻防演练热点事件
- 图2.毒云藤-利用保密竞赛热点事件

钓鱼邮件攻击中采用了大量诱饵文档，这些诱饵文档均为正常文件，大部分是目标官方网站公开文件，部分是未公开文件，我们怀疑是毒云藤组织在以往攻击活动中窃取的文档进一步作为诱饵文件。

相关诱饵文档基本都是通知公告类，进一步主要分为项目申请、政策文件、会议论坛、疫情防控这几类。



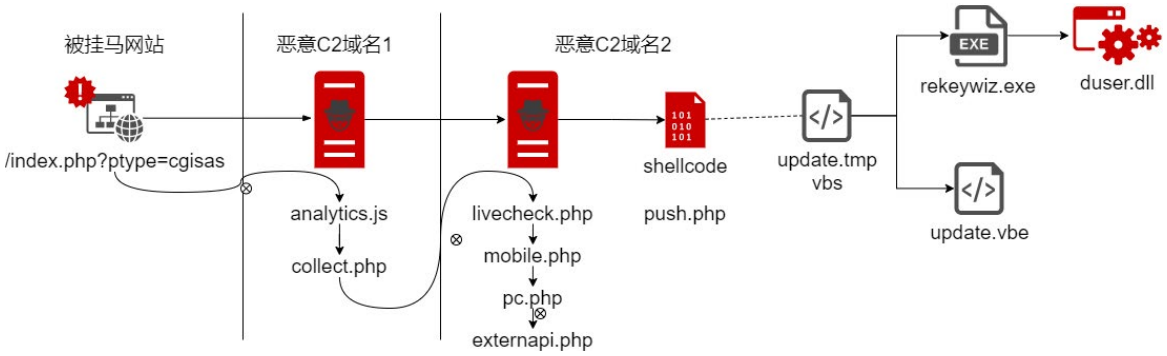
下表是攻击活动中部分诱饵文档名
市XX局-5g空间规划进展情况.docx
地方与外方签署的合作文件汇总表.xls
XXX2021年度部级法学研究课题指南.docx
202105发布的3批XXX重点专项-含通知.pdf
XXX重点发展评估申报表.doc
第十二届XXX电子展.rar
第六届XXX新材料大会通知.pdf

• 毒云藤诱饵文档类型

02.APT-C-06 (Darkhotel)

Darkhotel组织攻击活动最早可追溯到2010年，擅长利用浏览器漏洞，尤其是0day漏洞针对重点目标进行精准攻击。去年针对我国的攻击活动中就利用了浏览器、VPN的多个0day漏洞，今年也不例外，4月初我们监控发现了该组织发起了一次新的攻击活动。

这次是针对某网站挂马进行水坑攻击，该组织又一次利用了一个全新的IE浏览器0day漏洞（CVE-2021-34448[6]）。为了避免安全检测和其他非目标范围人群触发漏洞导致攻击暴露，整个水坑攻击过程中恶意脚本有多重验证由此筛选出真正的攻击目标并最终执行触发0day漏洞。最终释放的样本路径、样本中的混淆代码与thinmon攻击活动存在复用，且最终载荷与thinmon 的最终载荷一样都使用了metepreter服务端组件metsrv.dll。



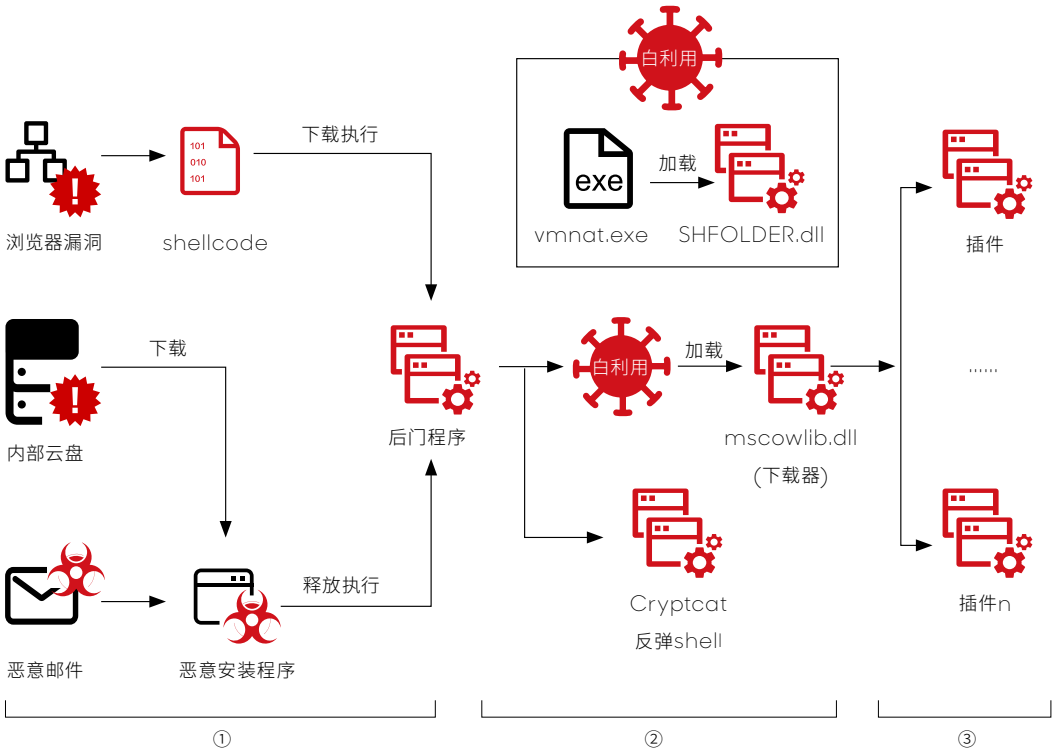
Darkhotel组织0day攻击流程

域名	文件名	响应行为
C&C-1	analytics.js	收集受害者的浏览器信息，发送到collect.php
	collect.php	跳转到livecheck.php
C&C-2	livecheck.php	访问mobile.php，并执行该页面返回的代码
	mobile.php	加密的js代码，解密后仍有部分乱码
	pc.php	加密的js代码，访问extrnapi.php
	externapi.php	编码的js漏洞代码，解码后执行

03.APT-C-59 (芜琼洞)

今年上半年我们捕获到一个未知组织针对我国科研、媒体和医疗卫生行业重点单位的一系列攻击活动，相关技战术均为全新首次应用，我们将这个全新组织命名为芜琼洞。该组织攻击活动最早是2020年8月至今非常活跃，该组织同样具备0day漏洞攻击能力，且习惯围绕时事热点针对特定目标展开定制化攻击。

在我们监控的三个被攻击目标中，该组织就采用了三种不同的攻击方式，1月利用IE浏览器0day漏洞（CVE-2021-26411）[7]针对我国科研机构发起定向攻击，另外值得注意的是同期Lazarus组织针对安全研究人员的攻击中也利用了该漏洞[8]；3月，基于目标内网环境进一步进行水坑攻击；5月，针对医疗卫生机构采用鱼叉邮件投放篡改后恶意安装包进行攻击。



步骤1：攻击者使用浏览器漏洞、水坑攻击、钓鱼邮件多种方式投递后门程序

步骤2：后门程序部署Cryptcat的修改版和下阶段载荷的下载器

步骤3：下载器下载各种插件实现具体的功能

• 芜琼洞三种攻击方式

04.其他

APT-C-26 (Lazarus) 上半年的攻击活动依然积极活跃，尤其是1月Google威胁分析小组披露的该组织利用社交媒体针对安全研究人员的攻击[9]，在我们进一步跟踪监控中发现该组织还利用了谷歌浏览器（CVE-2021-21148[10]）和IE浏览器（CVE-2021-26411[11]）两个 0day漏洞，其中关于芜琼洞组织也利用了IE浏览器0day漏洞，在上述章节已经提到。从攻击技术手法看，Lazarus擅长使用伪造的社交媒体进行社会工程学攻击，而此次的攻击者也在LinkedIn上冒充安全公司的招聘人员[12]，来吸引那些对漏洞利用和攻击感兴趣的安全人员。

今年的危险密码行动还在继续,利用区块链工作组机会等诱饵发起攻击，但攻击次数相较于去年已经大幅度降低。另外上半年Lazarus的子组织Andariel卷土重来，Andariel的攻击目标以韩国国防工业为主[13]，以窃取信息、间谍活动为目的。值得注意的是，今年的攻击活动中出现了勒索软件攻击。这并不是Lazarus组织首次涉及勒索软件，去年卡巴斯基披露了Lazarus组织运营的VHD勒索软件[14]。

APT-C-55 (Kimsuky) 2021上半年攻击频繁，攻击目标仍以韩国的政府外交、国防等。3月，我们披露了一批Kimsuky网络攻击武器与测试样本[15]，相较于历史攻击活动，这次更多的是利用第三方云盘和被黑网站作为攻击基础设施。上半年攻击活动仍以鱼叉邮件投递诱饵文档为主，同时也在积极利用社会热点事件为诱饵进行攻击。我们根据恶意脚本窃密攻击流程分为5类。

分类	利用诱饵类型	活跃时间
第一类（直接窃取）	问卷调查类文档为主	2020年11月-2021年3月
第二类（PowerShell）	社会时事热点为主	2020年6月至今
第三类（XML）	拜登政府政策、党军事题材为主	2020年12月至今
第四类（Google博客）	会议类、问卷类诱饵为主	2021年6月至今
第五类（Onedrive网盘）	测试文档为主	2020年12月-今

• Kimsuky组织5类恶意脚本窃密攻击流程

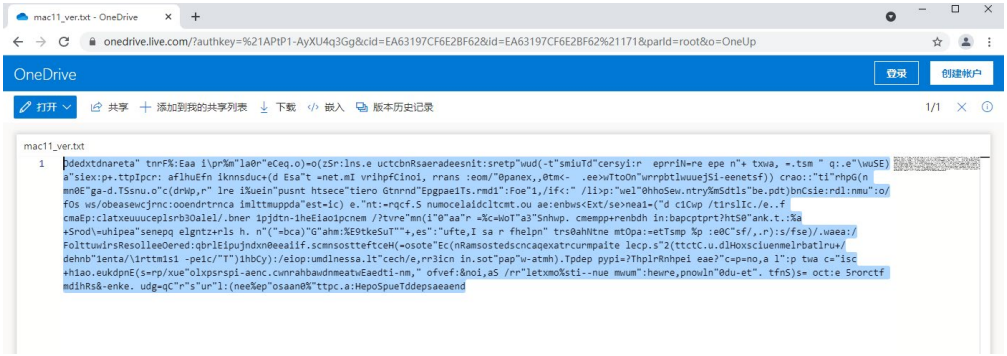


图1

APT-C-60（伪猎者）：该组织针对我国的攻击活动最早可以追溯到2018年，攻击活动一直持续至今，攻击目标主要以人力资源咨询和贸易相关单位为主。今年的攻击活动，是以鱼叉邮件投递恶意压缩包为主，主要针对目标发送伪装成简历的恶意文件，攻击成功驻留后持续使用WinRAR收集回传受害者敏感数据，以窃取敏感文档为主。

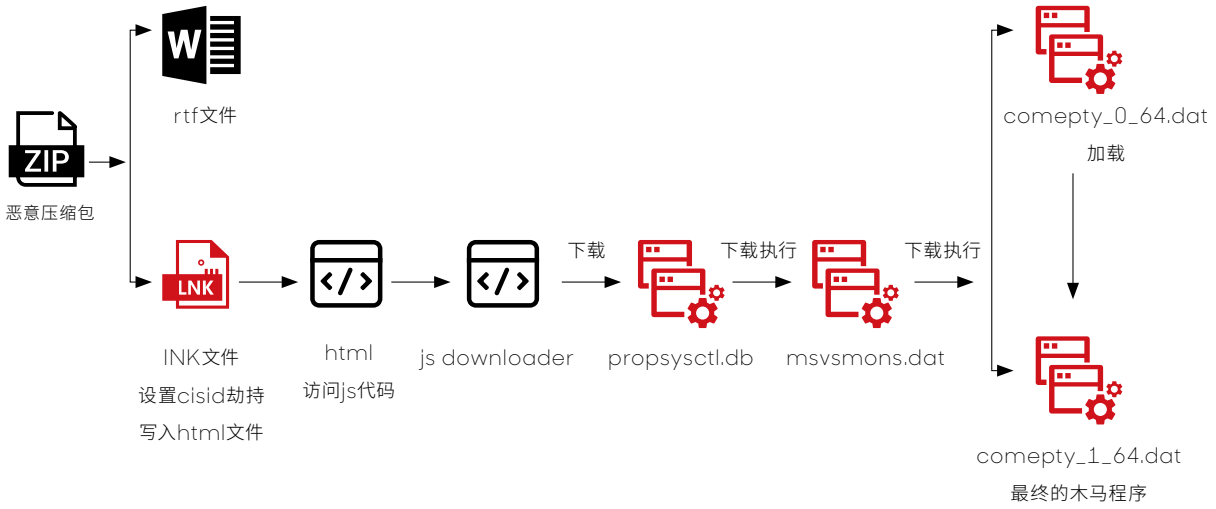


图2

- 图1.恶意Onedrive网盘
- 图2.伪猎者攻击流程

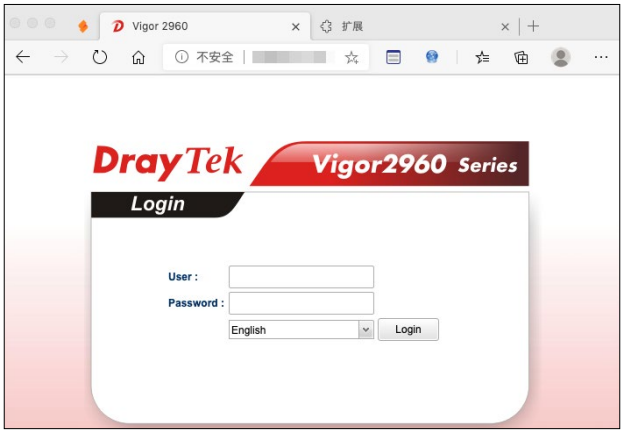
3.东南亚

01.APT-C-00 (海莲花)

2021年上半年，海莲花组织针对我国的攻击活跃程度较去年有所提升，攻击活跃程度仅次于毒云藤、蔓灵花，3月和4月攻击处于高峰。今年针对ICT供应商的攻击占比位居首位，已超过直接针对政府、教育等重点单位的攻击。这些目标供应商主要服务于国防、政府、教育、交通等多个领域。另外，海莲花较其他主流APT组织还有一个显著的区别，就是在初始攻击突破进入目标内网环境后，会进行大规模复杂的横向移动攻击。今年上半年继续沿用了去年主流的三种横向移动攻击手法：远程建立服务、远程调用WMI服务、控制内网安全软件服务端下发指令。

越来越多的被攻陷网络设备作为C2服务器，在去年的攻击活动中物联网设备已成为APT新的战备资源，海莲花组织也在积极尝试由此获得更多武器资源，去年7月，我们捕获到海莲花组织陆续攻击路由器设备，主要针对DrayTek厂商路由器设备，进一步将其作为流量中转跳板，相关攻击活动持续至今。

另外今年4月各单位展开实网攻防演练期间，海莲花攻陷了多个企业OA系统服务器，同样这些服务器仅作为C2跳板中转用。



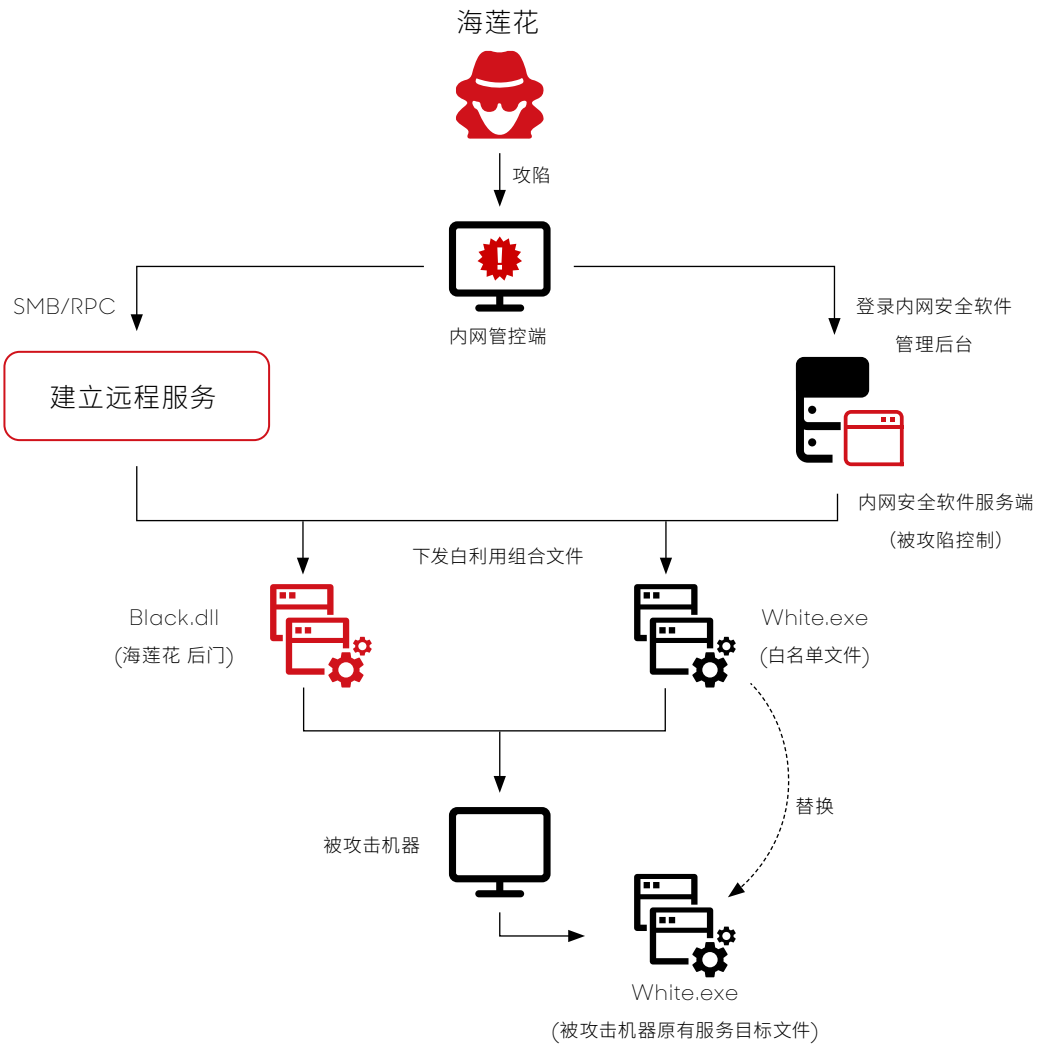
主流攻击：白利用+HiJack家族，海莲花的HiJack家族是目前最活跃的样本类型，该家族样本使用前期渗透侦查，获取到的被攻击机器的信息（IP、MAC地址等），以此当做高强度加密方法（AES / RC4）唯一的KEY，来解码恶意载荷，如果环境相关参数不匹配，则不执行恶意操作，增加安全软件检出难度和分析人员的分析难度。

• DrayTek路由器设备登录页面

白利用持久化新组合，根据360安全大脑观测到的数据，我们发现海莲花组织攻入企业内部后，滥用白利用技术，进行持久化驻留。海莲花组织实施横移技术以后，为了持久化驻留，使用了一个新的白利用驻留模式。

劫持已有软件服务项：搜集目标系统中可被劫持的目标服务项信息，将可被白利用的目标文件，替换目标服务项所属的主要工作组件。替换完毕后，可等待应用程序服务被动启动，也可通过SMB/RPC或内网安全软件服务端下发命令来远程启动此服务，从而实现后门模块持久化驻留系统。

此方式没有对服务项进行敏感操作，例如增加新服务项或修改原服务项，只对服务目标文件进行替换。可以理解为模拟常规软件的升级过程，替换被劫持服务的目标文件，替换后的目标文件依然为白名单文件。目的是为了躲避安全软件的筛查。



• 白利用持久化新组合攻击流程

02.APT-C-30（潜行者）

潜行者组织针对我国相关部门的攻击已经持续了12年左右，其攻击手法新颖、复杂，先后运用了NSA武器库、杀毒软件漏洞等先进攻击技术和大量对抗技术防止安全人员分析，攻击行动隐蔽低调，攻击周期长，是攻击能力出众的APT组织。

从2018年开始，360高级威胁研究院持续发现了潜行者组织相关最新攻击活动，被攻击者主要包括涉及政府、通信行业，而且该组织的目标范围主要集中在某几个重点单位，对目标的定向攻击方式和北美组织类似，与南亚地区组织差异较大。相关攻击最早可以追溯到2009年，攻击最早的样本编译时间为2008年，攻击活动一直持续至今。该组织对目标内网环境进行了深入研究，针对目标内网环境中的杀毒软件进行针对性的攻击，利用杀毒软件的升级服务漏洞植入后门，控制目标内网关键服务器并进行了持续的潜伏渗透。

今年上半年该组织主要针对东南亚地区通信行业相关单位，目的仍然以窃取重点单位敏感文件为主，攻击活动主要集中在1月至3月，其中攻击频率逐月递减。另外针对APT-C-30（潜行者）组织历年来攻击活动的技战术细节，我们近期将对外披露。

行动名称	时间	主要中招单位
FakeLon	2011 - 2013	涉及多个政府机构
NightCrawler	2011 - 2012	针对某政府机构
FakeKng	2009 - 2019	针对某政府机构
PackJet	2013 - 2015	针对某政府机构
SevenPack	2014 - 2019	针对某通信企业
KssLov	2016	涉及政府机构和通信企业
Fentel	2015 - 2020	多个领域，以通信为主
AIBD	2017 - 2020	针对某政府机构
YNN	2016 - 2021	涉及政府机构、通信、国防等

• 潜行者组织相关攻击行动汇总

多种横向移动方式

潜行者组织近10年来的后门的植入方式不尽相同，但多次攻击行动手法都有鲜明的技术特点，主要利用目标内网的杀毒软件漏洞进行攻击。攻击者在控制了目标内网的任意机器后,会利用杀软的漏洞攻击杀软的客户端和服务端,使该目标机器连接伪装的升级中心下载后门升级包并启动以植入后门，进一步后门会连接公网、内网的C&C，同时在受害者机器上添加管理员账号，开启文件共享，添加防火墙规则等弱化主机的防御，以便于攻击者稳固据点，在目标内网中再持续进行横向移动。

潜行者组织攻击的核心目标是长期控制并窃取敏感文件，一旦目标单位环境发生变化，如操作系统、防御体系更新升级等，都会及时采取应对措施。我们发现该组织在针对某单位横向移动过程中，该单位某杀毒软件多个版本（包括最新版本）都已被利用。

利用泄露的NSA武器库

除了使用杀软漏洞，潜行者组织还会使用Shadow Brokers在2017年4月14泄露的NSA武器库中的组件进行内网的横向移动。截至目前共捕获了三种武器组件Smbtouch-1.1.1、Doublepulsar-1.3.1、Eternalblue-2.2.0

名称	大小	压缩后大小	修改时间
eb.xml	7 636	1 504	2016-01-21 18:28
lists.exe	4 980 736	2 517 568	2016-01-21 19:27
liste.exe	4 980 736	2 499 344	2016-01-23 17:44
listd.exe	6 815 744	3 005 424	2016-01-23 17:56
dp.xml	5 182	1 248	2017-04-21 07:56
st.xml	4 924	1 264	2017-04-21 08:50
Hmmapi.dll	46 080	21 024	2017-05-02 09:26

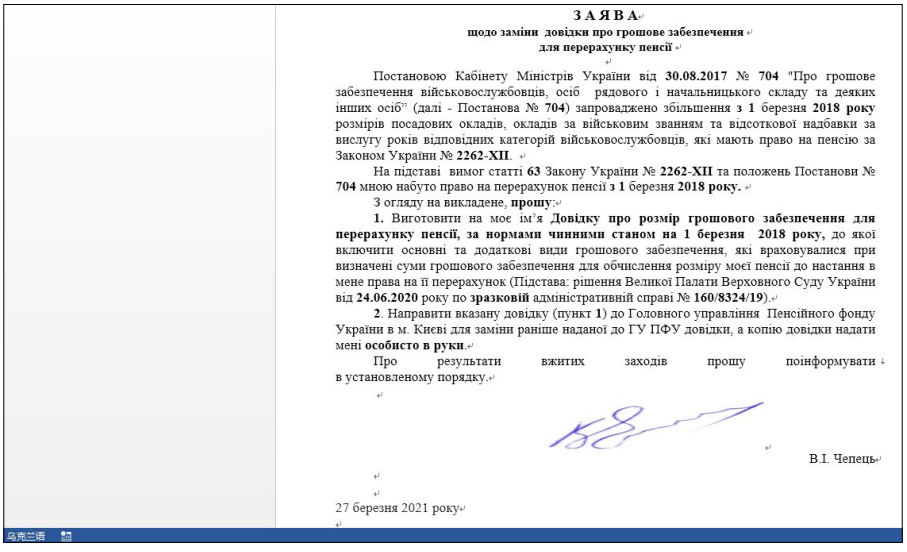
• 相关NSA武器库压缩包文件

4.东欧

东欧相关APT组织一直以来以欧美各国军政机构和一些重点企业为目标进行着持续不断的攻击活动，去年12月，震惊全球的SolarWinds供应链攻击活动就被发现与俄语系APT组织Turla的Kazuar相关组件存在关联。今年上半年Gamaredon组织最为活跃，另外APT28、APT29、Turla等组织今年也被披露有新的攻击活动。

01.APT-C-54 (Gamaredon)

作为最活跃的俄语系APT组织之一，Gamaredon一直以来的主要攻击对象为乌克兰的政府官员、新闻工作者和反对党成员，其攻击武器五花八门，擅长利用混淆后的vba宏、vbs及bat脚本进行攻击载荷的释放。今年5月，我们披露了Gamaredon新启用的一批后门程序，这些后门主要功能依旧是窃取目标计算机的特定格式文件，但相较于老版本的dll后门，新版本更新并完善了一些功能，且具有更强的隐蔽性。自今年年初俄乌关系不断恶化以后，Gamaredon组织加强了对乌克兰政府及军事机构目标的攻击，在此期间我们捕获到了大量来自该组织的诱饵文档，文档的语言均为乌克兰语。



З А Я В А

щодо заміни довідки про грошове забезпечення для перерахунку пенсії

Постановою Кабінету Міністрів України від **30.08.2017** № **704** "Про грошове забезпечення військовослужбовців, осіб рядового і начальницького складу та деяких інших осіб" (далі - Постанова № **704**) запроваджено збільшення **з 1** березня **2018 року** розмірів посадових окладів, окладів за військовим званням та відсоткової надбавки за вислугу років відповідних категорій військовослужбовців, які мають право на пенсію за Законом України № **2262-XII**.

На підставі вимог статті **63** Закону України № **2262-XII** та положень Постанови № **704** мною набуто право на перерахунок пенсії **з 1** березня **2018 року.**

З огляду на викладене, **прошу**:

1. Виготовити на моє ім'я **Довідку про розмір грошового забезпечення для перерахунку пенсії, за нормами чинними станом на 1 березня 2018 року,** до якої включити основні та додаткові види грошового забезпечення, які враховувалися при визначені суми грошового забезпечення для обчислення розміру моєї пенсії до настання в мене права на її перерахунок (Підстава: рішення Великої Палати Верховного Суду України від **24.06.2020** року по **зразковій** адміністративній справі № **160/8324/19**).

2. Направити вказану довідку (пункт **1**) до Головного управління Пенсійного фонду України в м. Києві для заміни раніше наданої до ГУ ПФУ довідки, а копію довідки надати мені **особисто в руки**.

Про результати вжитих заходів прошу поінформувати в установленому порядку.

В.І. Чепець

27 березня 2021 року

乌克兰语

• Gamaredon组织使用的诱饵文档

持续跟踪Gamaredon组织的相关活动时，发现该组织利用修改PE文件的方式向带有合法签名的PE文件中嵌入恶意脚本[16]。虽然向数字证书中嵌入payload的手法早已被披露，但是该组织利用此种手法执行vbs还是首次出现。

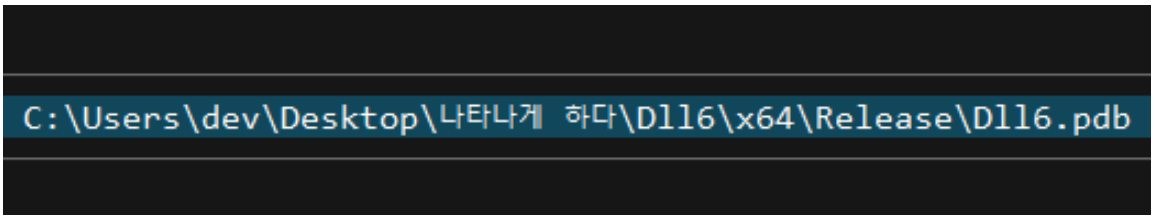
02.其他

APT-C-20 (APT28)：是具有俄罗斯背景的APT组织中较为活跃的一个，该组织的zebrocy家族木马在近几年的攻击活动中尤其活跃，该组织也一直保持着该家族的更新，目前已知的该家族样本包括delphi、go、nim等版本。去年年底，我们披露了该组织新版zebrocy的相关活动。今年2月公开情报披露了一起疑似APT28组织针对哈萨克斯坦高碳铬铁生产商Kazchrome的攻击活动[17]，攻击者通过诱饵文档引诱受害者启用宏并释放执行攻击载荷。该载荷采用delphi语言编写，易让人联想起同样采用delphi语言版本的zebrocy downloader，但由于编译器版本差异和代码架构差异过大，且后续没有发现更多相关活动，本次攻击活动是否归属于APT28组织还需持续跟踪研判。

• 篡改后的Chrome.exe并保持数字签名的有效性

APT-C-25 (APT29)：一直以来被指与俄罗斯对外情报部门存在关联，多次以美国和欧洲国家为目标，通过爆破密码和邮件钓鱼等方式进行网络攻击，该组织具备0day作战能力，且行动较为隐蔽。

今年5月，国外安全厂商Volexity[18]监控到一起该组织针对多国政府机构的邮件钓鱼活动，该组织利用钓鱼邮件中的诱饵文档释放并执行恶意程序。有趣的是，相关恶意文件中故意留下了包含韩语的路径字符串，疑似用于误导安全研究员。



APT-C-29 (Turla)：是众多俄语系APT组织中，所掌握武器和利用方式最复杂的组织之一，该组织的Carbon、ComRat、Karzuar等后门套件，不仅功能丰富且易于扩展，长期以来也保持着更新和版本迭代，去年年末，震惊全球的solarwinds事件就被指与该组织的Karzuar后门存在关联。

今年年初，国外的安全研究者发现该组织开始将Iron Python纳入自身攻击武器的一环，通过给受害者计算机安装Iron Python，Turla组织成员得以运行python编写的恶意脚本，且能在python代码中直接调用.net平台的API，功能十分强大。从这一点来看，该组织未来可能会利用各式各样的脚本解释器进行恶意活动。

• 包含韩语字符串的PDB路径

发布时间	攻击事件	发布机构
1月5日	FBI、CISA、ODNI、NSA关于Solarwinds事件的联合声明[19]	CISA
2月15日	Sandworm组织攻击法国开源IT监控系统[20]	CERT-FR
2月19日	IronNetInjector: Turla的新恶意软件加载工具[21]	Palo Alto Networks
2月22日	疑似APT28利用高碳铬铁生产商登记表为诱饵的攻击活动分析[22]	奇安信
3月7日	与俄罗斯有关的APT组织利用立陶宛基础设施发动攻击[23]	Security Affairs
4月15日	“雏莺行动”：一起针对俄罗斯的窃密行动[24]	安天
4月15日	美国政府确认SolarWinds攻击者是俄罗斯SVR[25]	FBI
4月26日	俄罗斯情报局 (SVR) 攻击行动：趋势及防御[26]	US-CERT
5月3日	鱼叉攻击使用COVID诱饵瞄准乌克兰政府[27]	Fortinet
5月27日	疑似APT29进行了以选举欺诈为主题的网络钓鱼活动[28]	Volexity
6月4日	SBU阻止了俄罗斯特种部队针对乌克兰当局计算机网络的大规模网络攻击[29]	乌克兰安全局
6月25日	新的Nobelium活动[30]	Microsoft

5.中东

中东地区局势动荡复杂，黑天鹅事件频发，2021年4月，伊朗的纳坦兹核设施电力系统疑似遭到以色列的电子攻击出现问题，伊朗是中东网络攻击活动的首要目标，2021年上半年中东地区多个组织攻击活动频繁，最活跃的要属于MuddyWater，APT34、Charming Kitten也多次被披露，2021年中东地区的攻击仍然是以政治主题为主，同时伊朗组织Charming Kitten的目标开始转向医学人员。

01.MuddyWater

MuddyWater攻击组织，其攻击目标包括伊拉克、约旦、土耳其等中东地区国家，具有较明显的政治意图，其使用最多的方式是钓鱼文档，并最终将PowerShell后门植入到目标机器上。善于利用各种脚本后门，并且会对脚本添加复杂的混淆，加大了攻击监测难度，也增加了对于攻击样本的分析难度。

MuddyWater是今年上半年中东地区最活跃的攻击者，使用的攻击方式都比较新颖，先是被发现利用了github托管Cobalt Strike脚本[31]，随后其在用以色列的地缘政治为主题的攻击行动中使用Onehub作为载体[32]。使用的恶意文档以及翻译后的图片如下:

السادة الأفاضل / منسوبي الجهات الحكومية
كل عام وأنتم بخير
بعد تحية طيبة ،،،
بالنظر إلى الأوضاع في المنطقة خاصة بعد الانتخابات الأمريكية والمخاوف بشأن أفعال إيران، تم إجراء دراسات مشتركة بين المجلس الوطني للإعلام و الأمانة العامة لمجلس التعاون لدول الخليج العربية حول إحصاء العواقب السياسية والأمنية والاقتصادية لتطبيع العلاقات بين الدول العربية وإسرائيل.
وبالتالي لقد تم تقديم مسودة الدراسات الخاص بمفاوضات حول تطبيع العلاقات بين الدول العربية وإسرائيل من قبل خبراء الدول الاعضاء بالأمانة العامة لمجلس التعاون لدول الخليج العربية، و في هذا الصدد، تسعى المجلس الوطني للإعلام إلى إجراء استطلاع شامل من قبل الدول الأعضاء.
قم بتنزيل المحتوى ذي الصلة عبر الرابط أدناه.
تحليل ودراسة / تطبيع العلاقات / الدول العربية واسرائيل /
https://nmc.gov.ae
و تفضلوا بفائق الاحترام

尊敬的先生/政府官员
大家都很好。
在亲切的问候之后，
鉴于该地区的局势，特别是美国选举后的局势和对伊朗行动的关切，国家新闻委员会和海湾合作委员会秘书处进行了联合研究。统计阿拉伯国家和以色列关系正常化的政治、安全和经济后果。因此，海湾合作委员会秘书处成员国专家提交了关于阿拉伯国家与以色列关系正常化谈判的研究报告草稿。在这方面，国家新闻委员会寻求会员国进行全面调查。
通过下面的链接下载相关内容。
对阿拉伯国家/以色列关系正常化的分析和研究https://nmc.gov.ae
请恕我直言。

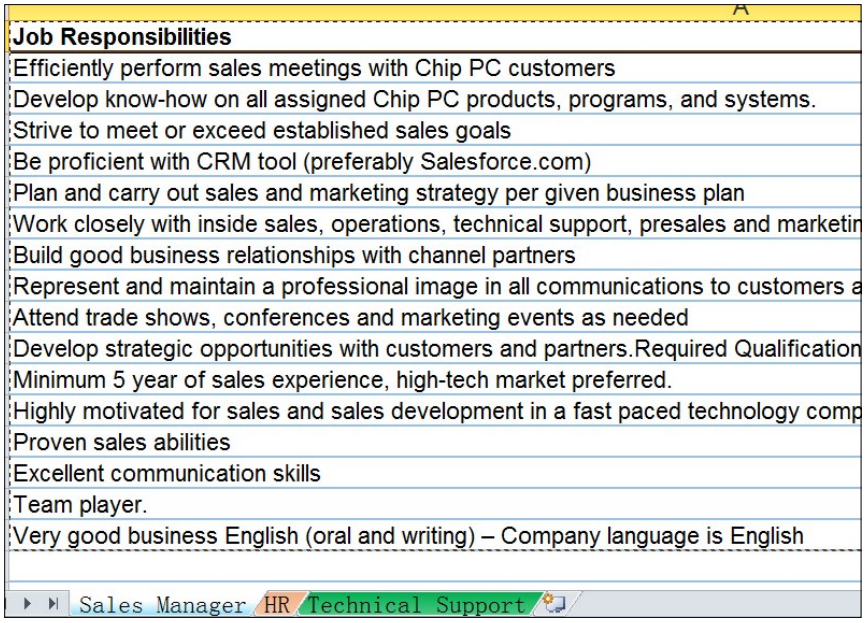
• 恶意文档以及翻译后的图片

02.Oilrig

Oilrig组织，也被称为APT34，最早于2017年1月以GreenBug命名被首次公开披露，Oilrig以电信、石油和航空业为攻击目标，主要针对美国、欧洲和中东地区。

该组织使用自定义的RDAT后门，RDAT自2017年到2019年一直被长期维护，该工具的主要特点是http和dns隧道的通信，多种变体也都依赖于http和dns隧道进行网络通信。自2019年一个名为“Lab Dookhtegan”的实体泄漏APT34工具以来，该组织一直在对攻击组件持续开发和更新，以便更隐秘的进行新一轮的活动，tonedeaf类型恶意软件就在这之后被发现。在2020年4月、5月针对中东、南亚的电信提供商进行了攻击中使用了自定义 Mimikatz 工具。

特别是在今年，OilRig被发现疑似采用了新的后门变体SideTwist针对黎巴嫩相关目标[33]，该组织的武器库得到了进一步的更新。OilRig在最近的攻击中特别多的使用求职、应聘作为恶意文档的关键字，我们此次捕获到的疑似恶意文档打开后内容也是一个招聘信息，描述的工作内容与芯片PC产品、程序和系统相关，需要销售经理、HR、技术支持三个岗位，看似与工作相关，实则是迷惑相关人员。下图为此次攻击捕获的文档截图：



A
Job Responsibilities
Efficiently perform sales meetings with Chip PC customers
Develop know-how on all assigned Chip PC products, programs, and systems.
Strive to meet or exceed established sales goals
Be proficient with CRM tool (preferably Salesforce.com)
Plan and carry out sales and marketing strategy per given business plan
Work closely with inside sales, operations, technical support, presales and marketin
Build good business relationships with channel partners
Represent and maintain a professional image in all communications to customers a
Attend trade shows, conferences and marketing events as needed
Develop strategic opportunities with customers and partners.Required Qualification
Minimum 5 year of sales experience, high-tech market preferred.
Highly motivated for sales and sales development in a fast paced technology comp
Proven sales abilities
Excellent communication skills
Team player.
Very good business English (oral and writing) – Company language is English

Sales Manager | HR | Technical Support

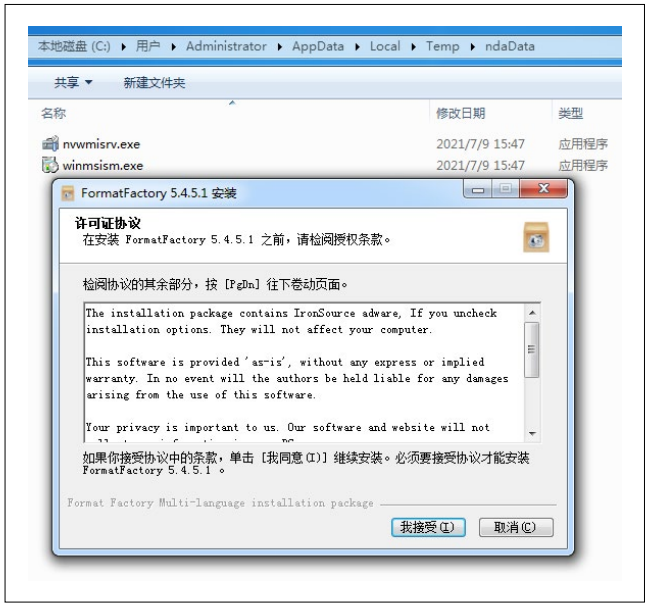
• OilRig组织诱饵文档

03.其他

APT-C-41（蓝色魔眼）又称StrongPity，其攻击活动主要针对比利时、叙利亚等国家进行，去年年底我们也发现了该组织针对我国的攻击行动。

该组织攻击武器复杂而丰富，拥有0day作战的能力，且一直保持着武器库的更新迭代，擅长利用携带后门的恶意安装包进行水坑攻击。WinRAR、7-ZIP、TeamViewer等常用的软件安装包都被该组织利用过。

今年2月至4月，我们捕获到若干该组织制作的恶意安装包，被伪装的软件类型包括Skype、Winrar、Find And Mount等，其中我们发现了该组织针对国内软件格式工厂，制作了恶意安装包，但我们暂时没有在国内发现相关活动。



APT-C-23（双尾蝎）首次发现该组织定制的iOS监控软件[34]，该组织通过诱骗安装移动配置文件的方式，在不需要越狱设备安装特定于设备的签名版本的iOS应用程序。安装后，恶意软件利用了Sock Port漏洞越狱以提升其权限，以获取无法通过标准 iOS 权限请求访问的敏感用户信息。同时，还发现该组织使用庞大的基础设施来支持其运营，其中包括 100多个托管iOS和Android恶意软件，试图通过网络钓鱼窃取凭据或充当命令和控制服务器的网站。

• 运行合法格式工厂安装包的同时释放后门文件

PART 03

2021上半年攻击态势总结

1.全球疫情严峻形势下境外APT组织针对我国的攻击持续活跃

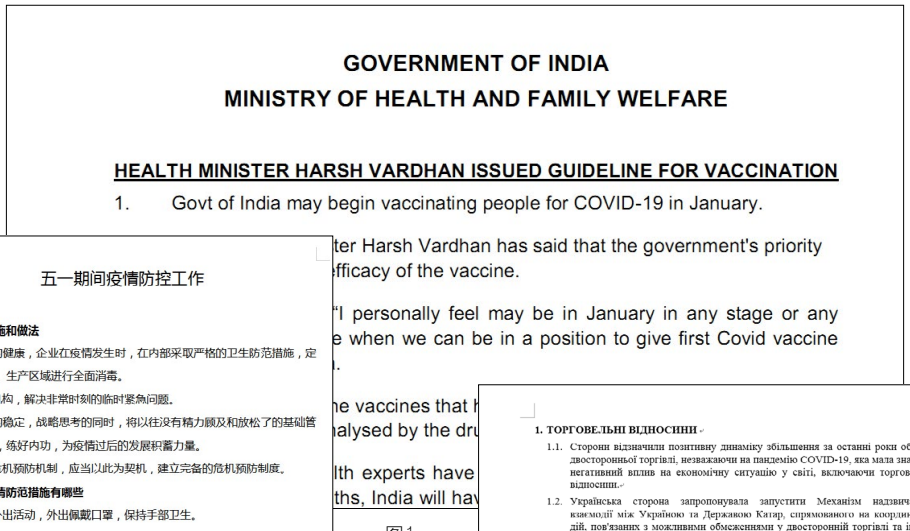
01.围绕“新冠疫情”相关攻击活动依然处于高位

今年上半年全球新冠肺炎疫情形势依然严峻，截至7月1日，累计病例已超1.8亿例。如南亚地区多国疫情反复爆发。这期间内围绕“新冠疫情”相关攻击活动依然处于高位，主要体现在利用新冠疫情作为诱饵社工、攻击医疗行业企业和政府监管机构。

4月，我们披露了透明部落组织利用疫情相关信息对印度医疗行业进行情报窃取的定向攻击活动[35]。5月，芜琼洞、蔓灵花组织先后针对我国医疗机构发起了定向攻击。

APT组织	利用新冠诱饵文档	攻击医疗机构	攻击政府机构
APT-C-00 (海莲花)		是	
APT-C-01 (毒云藤)	是	是	
APT-C-08 (蔓灵花)	是	是	是
APT-C-24 (响尾蛇)		是	是
APT-C-28 (Scarcruft)	是		
APT-C-54 (Gamaredon)	是		
APT-C-55 (Kimsuky)	是		
APT-C-56 (透明部落)	是	是	
APT-C-59 (芜琼洞)			是

• 围绕“新冠疫情”攻击活动涉及的部分APT组织



GOVERNMENT OF INDIA
MINISTRY OF HEALTH AND FAMILY WELFARE

HEALTH MINISTER HARSH VARDHAN ISSUED GUIDELINE FOR VACCINATION

1. Govt of India may begin vaccinating people for COVID-19 in January.

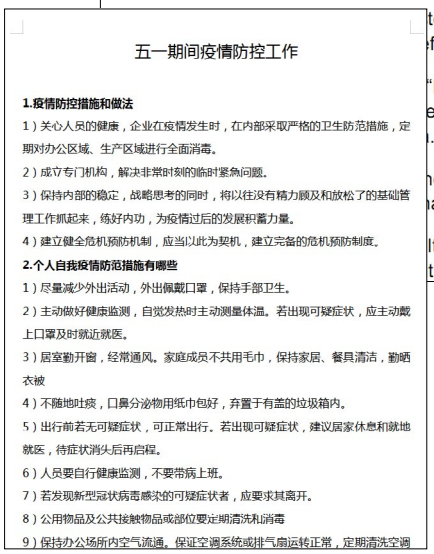
ter Harsh Vardhan has said that the government's priority
fficacy of the vaccine.

"I personally feel may be in January in any stage or any
e when we can be in a position to give first Covid vaccine
.

he vaccines that
nalysed by the dr

lth experts have
ths, India will ha

图1



五一期间疫情防控工作

1.疫情防控措施和做法

1）关心人员的健康，企业在疫情发生时，在内部采取严格的卫生防范措施，定期对办公区域、生产区域进行全面消毒。

2）成立专门机构，解决非常时刻的临时紧急问题。

3）保持内部的稳定，战略思考的同时，将以往没有精力顾及和放松了的基础管理工作抓起来，练好内功，为疫情过后的发展积蓄力量。

4）建立健全危机预防机制，应当以此为契机，建立完备的危机预防制度。

2.个人自我疫情防范措施有哪些

1）尽量减少外出活动，外出佩戴口罩，保持手部卫生。

2）主动做好健康监测，自觉发热时主动测量体温。若出现可疑症状，应主动戴上口罩及时就近就医。

3）居室勤开窗，经常通风。家庭成员不共用毛巾，保持家居、餐具清洁，勤晒衣被

4）不随地吐痰，口鼻分泌物用纸巾包好，弃置于有盖的垃圾箱内。

5）出行前若无可疑症状，可正常出行。若出现可疑症状，建议居家休息和就地就医，待症状消失后再启程。

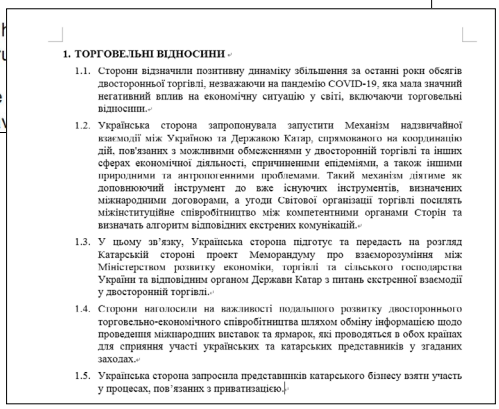
6）人员要自行健康监测，不要带病上班。

7）若发现新型冠状病毒感染的可疑症状者，应要求其离开。

8）公用物品及公共接触物品或部位要定期清洗和消毒

9）保持办公场所内空气流通。保证空调系统或排气扇运转正常，定期清洗空调

图2



1. ТОРГОВЕЛЬНІ ВІДНОСИНИ

1.1. Сторони відзначили позитивну динаміку збільшення за останні роки обсягів двосторонньої торгівлі, незважаючи на пандемію COVID-19, яка мала значний негативний вплив на економічну ситуацію у світі, включаючи торговельні відносини.

1.2. Українська сторона запропонувала запустити Механізм надзвичайної взаємодії між Україною та Державою Катар, спрямованого на координацію дій, пов'язаних з можливими обмеженнями у двосторонній торгівлі та інших сферах економічної діяльності, спричиненими епідеміями, а також іншими природними та антропогенними проблемами. Такий механізм діятиме як доповнюючий інструмент до вже існуючих інструментів, визначених міжнародними договорами, а угоди Світової організації торгівлі посилять міжінституційне співробітництво між компетентними органами Сторін та визначать алгоритм відповідних екстрених комунікацій.

1.3. У цьому зв'язку, Українська сторона підготує та передасть на розгляд Катарській стороні проект Меморандуму про взаєморозуміння між Міністерством розвитку економіки, торгівлі та сільського господарства України та відповідним органом Держави Катар з питань екстреної взаємодії у двосторонній торгівлі.

1.4. Сторони наголосили на важливості подальшого розвитку двостороннього торговельно-економічного співробітництва шляхом обміну інформацією щодо проведення міжнародних виставок та ярмарок, які проводяться в обох країнах для сприяння участі українських та катарських представників у згаданих заходах.

1.5. Українська сторона запросила представників катарського бізнесу взяти участь у процесах, пов'язаних з приватизацією.

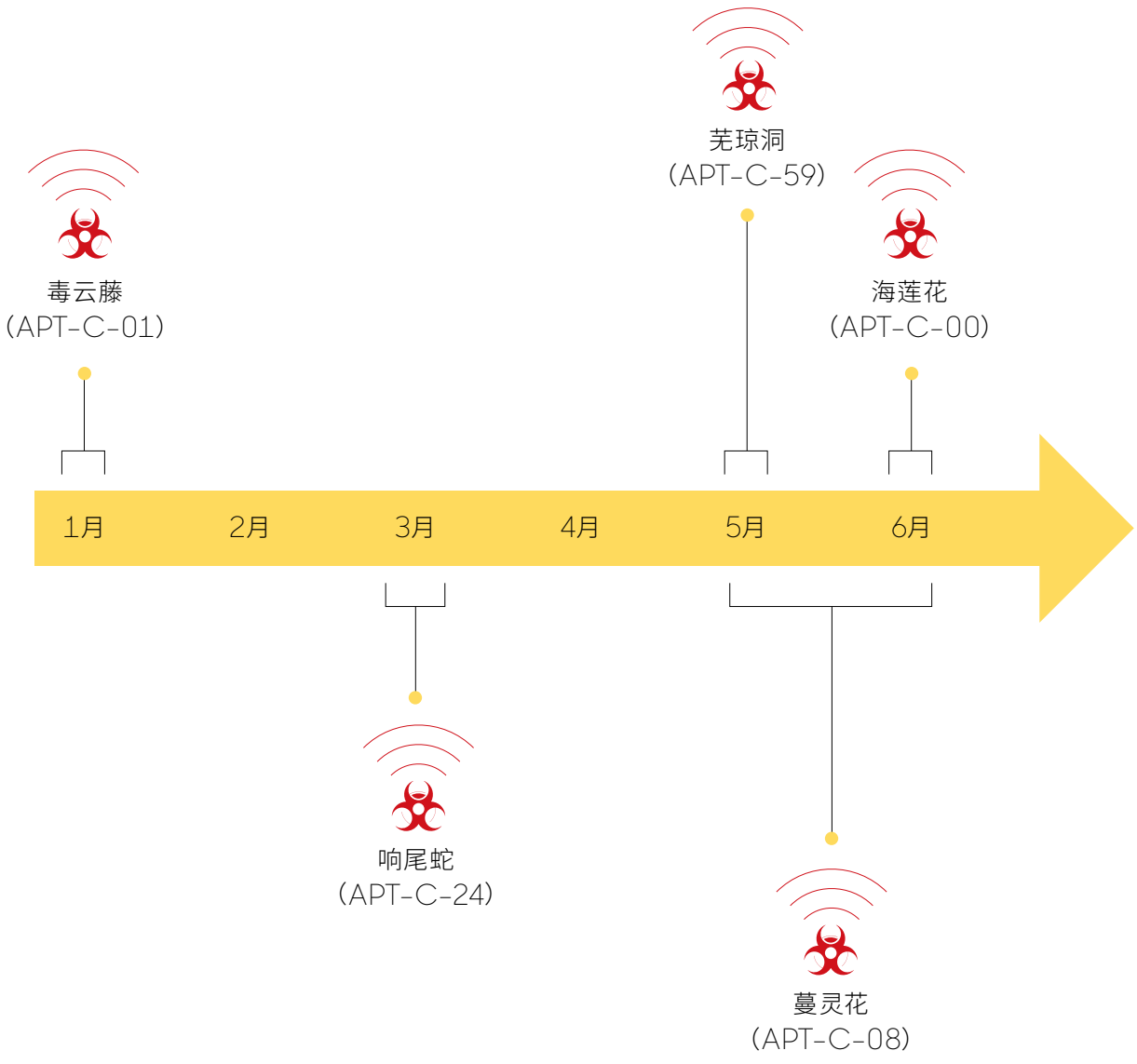
图3

部分诱饵文档文件名：
五一期间疫情防控工作.docx
防疫重点.rar
신종_코로나바이러스_관련_소상공인_지원_종합안내.hwp (新_冠状病毒_相关_小型企业_支持_综合指南.hwp)
COVID Vaccination for All Employees.pdf
疫情津贴启动信息.chm
免疫灭活疫苗的研制汇总表.doc
近期开展新冠疫情防控工作情况.docx
附件1.重点保障人群新冠疫苗紧急使用接种需求登记表（加入接种门诊）.xlsx
Pyongyang stores low on foreign goods amid North Korean COVID-19 paranoia (1).doc

• 图1.透明部落诱饵文档 • 图2.毒云藤诱饵文档 • 图3.Gamaredon诱饵文档

02.南亚、东南亚地区疫情严重，针对我国医疗机构APT攻击活跃

针对我国医疗卫生行业的攻击从去年疫情爆发就开始不断升温，如去年年初CNC、海莲花等组织针对我国多个医疗行业单位展开定向攻击活动。今年也不例外，4月，南亚等地区疫情蔓延爆发，5月开始南亚地区相关组织整体攻击活动有所放缓，但陆续出现多起针对我国医疗卫生机构的攻击活动，如蔓灵花、芜琼洞、海莲花等多个组织，针对医疗卫生行业的攻击陆续活跃。



• 针对我国医疗机构的部分APT组织

2.APT攻击紧跟时事热点

APT组织紧密围绕政治、经济等热点领域及事件的攻击活动，并不仅仅是利用作为诱饵钓鱼攻击用，更多是瞄准了涉及相关时事热点的重点机构或个人。

时事热点的范畴除政治、经济领域外，如疫情态势、某行业专项活动等都会被APT攻击所关注，尤其在今年上半年的攻击活动中，针对时事热点的跟进频次和细分粒度已明显超过去年同期。

图1

图2

- 图1.利用“办理2020年个税”诱饵
- 图2.毒云藤仿冒“保密观”的恶意安卓应用

A 12月

某交通行业集中整治工作的通知

毒云藤针对多个交通行业重点单位集中攻击

A 1月-2月

B 1月

拜登当选美国总统

芜琼洞针对我国外交、媒体等领域

B 1月下旬-2月初

C 3月1日-6月30日

个税申报

毒云藤以“办理2020年个税”诱饵，攻击多个行业单位

C 4月-5月

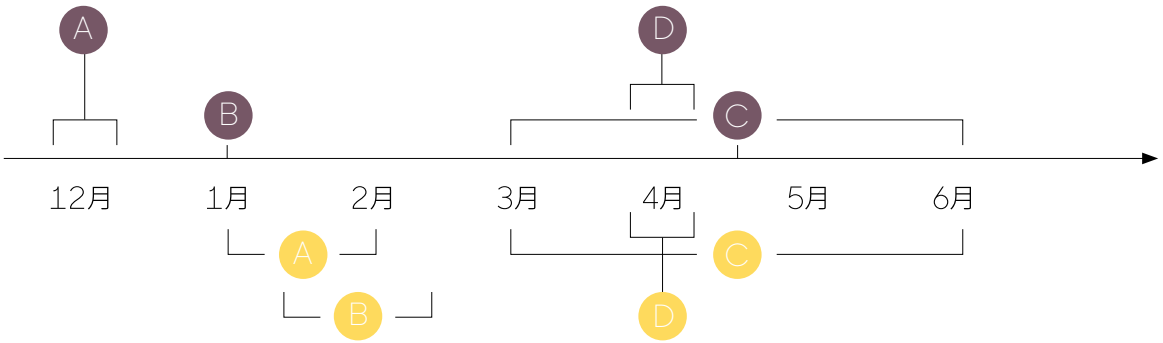
D 4月

各地展开实网攻防演练

毒云藤以攻防演练诱饵攻击；

海莲花针对某OA系统攻击；

D 4月



E 4月-5月

某知识竞赛活动

毒云藤钓鱼网站攻击和针对安卓移动平台攻击

E 4月

F 4月-5月

南亚新冠疫情爆发

蔓灵花、海莲花和芜琼洞针对医疗机构

F 5-6月

G 5月

5.1劳动节假期

毒云藤以“五一疫情防控”针对智库

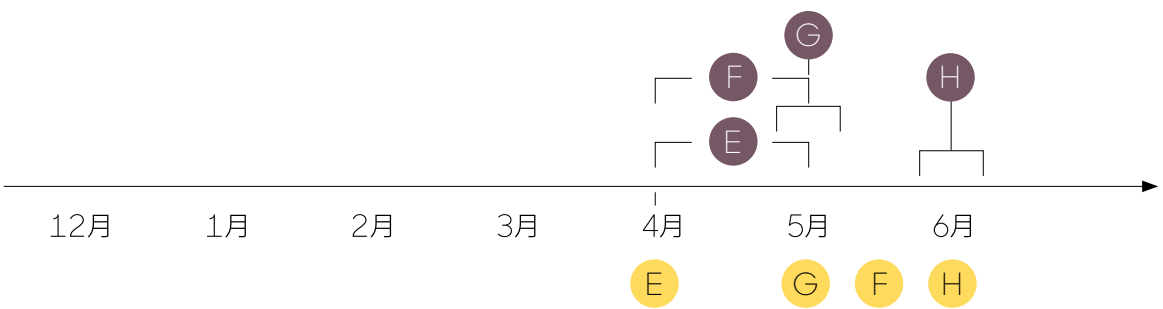
G 5月

H 6月

我国航天热点时事

CNC针对航空航天领域攻击

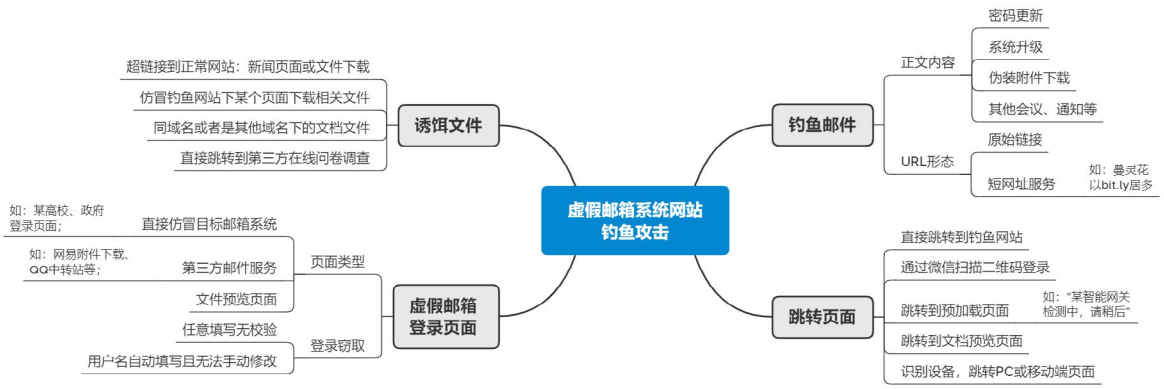
H 6月



3.仿冒目标单位邮箱系统集中钓鱼攻击频发

今年上半年的攻击活动中，初始攻击环节主要还是以钓鱼邮件攻击为主，进一步其中大部分是仿冒目标单位邮箱系统的钓鱼网站攻击。毒云藤今年的攻击活动基本都是这类钓鱼攻击，蔓灵花大部分也是基于此类。该阶段基本是无样本实体文件的钓鱼攻击，通过社会工程学直接窃取目标用户邮箱账号和密码，待进一步评估分析后会针对高价值目标继续投递木马恶意文件。

年初我们协助某客户取证分析时发现，访问钓鱼网站的用户中有近3成都填写了账号密码，如此高成功率和邮箱本身就包含了大量敏感文件信息，这样“高性价比”是APT组织得以青睐的主要原因，但这种攻击方式的弊端很明显，就是攻击活动非常容易暴露。



基于近一年我们捕获到的钓鱼网站攻击进行统计分析，主要的攻击环节如上图四部分：首先构造钓鱼邮件，进一步访问时会涉及跳转页面，具体仿冒邮箱系统的虚假登录页面会涉及多种，最后用户填写完账号密码后则展示相关诱饵文件。

基本大部分APT组织的钓鱼网站攻击都会涉及上述关键环节，具体类型会有较大差异，如今年的攻击活动中，钓鱼邮件中嵌套的钓鱼URL地址，蔓灵花会将其转换为bit.ly短网址，而毒云藤则保留原始URL链接形态；另如在用户被诱导填写账密过程，大部分情况用户名可以任意填写，但毒云藤在针对部分目标时，参数中自动填写登录用户名，而无法手动修改。

钓鱼攻击中邮件正文诱饵内容会千变万化，钓鱼网站也会不断更新迭代，但如果我们在查收邮件的过程中加以注意和防范，则可以鉴别出大部分钓鱼攻击和虚假网站。

• 仿冒目标单位邮箱系统主要攻击环节

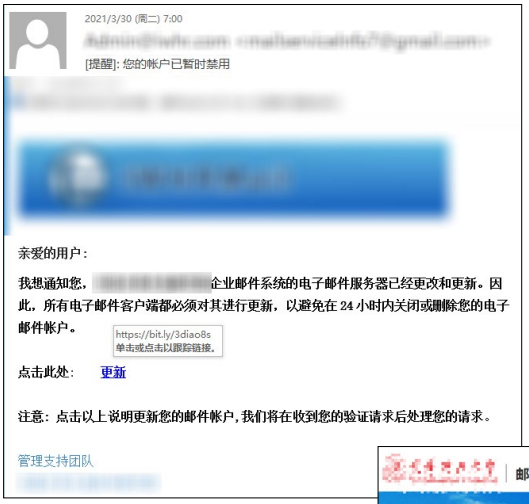


图1

图2

图3

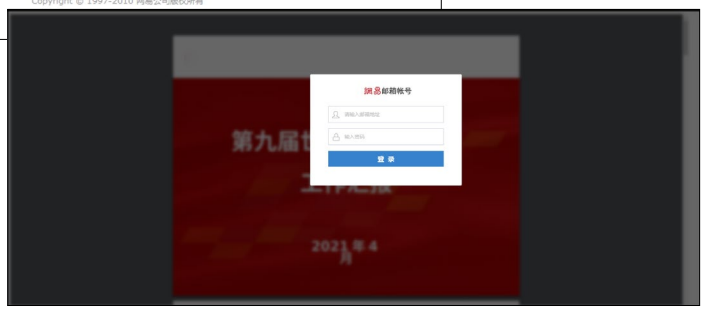


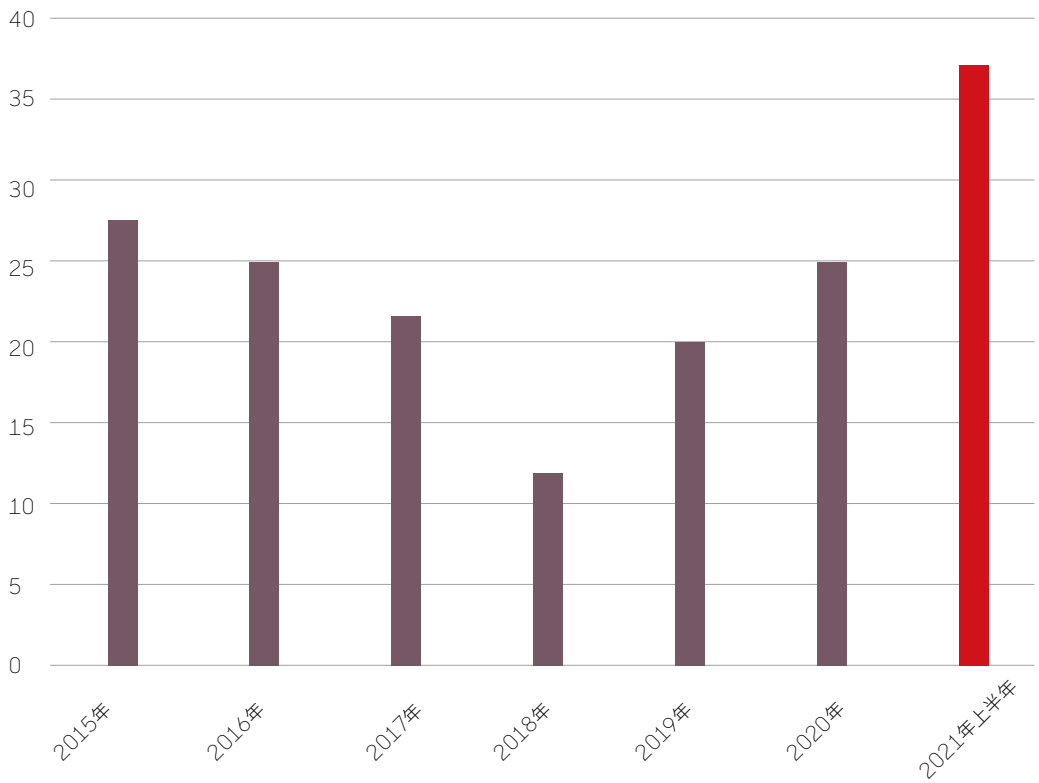
图4

- 图1.蔓灵花组织钓鱼邮件
- 图2.毒云藤组织仿冒某高校邮箱系统
- 图3.毒云藤组织仿冒邮箱附件预览页面
- 图4.蔓灵花组织仿冒某科研机构文件预览页面

4.2021上半年0day漏洞攻击频发

今年APT攻击活动中0day漏洞的使用较去年大幅增加，基于Google Project Zero项目统计，今年上半年利用的漏洞数量不仅已超2020年全年的总量[36]，而且达到历史新高。

从年初Lazarus组织利用谷歌浏览器（CVE-2021-21148）和IE浏览器（CVE-2021-26411）两个 0day漏洞，针对安全研究人员发起定向攻击；蔓灵花组织今年被披露利用0day漏洞（CVE-2021-1732）攻击活动；4月初，我们再次捕获到Darkhotel组织利用了一个全新的IE浏览器0day漏洞（CVE-2021-34448）。中旬，我们捕获到一起疑似半岛组织利用iOS 0day漏洞攻击（CVE-2021-30661、CVE-2021-30665、CVE-2021-30666）。我们可以看出相关0day漏洞攻击活动，不仅出现在如Darkhotel这类有丰富0day储备的组织，还是如蔓灵花组织今年首次被披露利用0day漏洞，或是如芜琼洞这类首次被发现的新组织。这也体现了APT组织整体攻击能力再不断提升加强。



• 攻击活动中利用在野0day漏洞数量（2015年-2021年上半年）

01.0day漏洞之间的争夺战

在本报告介绍东亚地区相关组织的攻击活动中，我们提到芜琼洞组织今年1月利用IE浏览器0day漏洞（CVE-2021-26411）针对我国科研机构发起定向攻击，另外值得注意的是同期Lazarus组织针对安全研究人员的攻击中也利用了该漏洞[37]。

结合公开数据分析如下表，我们发现Lazarus和芜琼洞几乎同一时期发起攻击，这在利用0day漏洞攻击事件中还是属于比较罕见的，我们无法确定该漏洞最初来源，不排除是由0day漏洞军火供应商同时提供给这两个组织，也有可能某组织在首次利用过程中被另一组织截获加以利用。

时间	事件	涉及组织	披露或发现机构
1月25日	利用社交媒体针对安全研究人员的攻击，仅提到chrome漏洞，并未提到IE	Lazarus	Google
1月26日	芜琼洞组织利用CVE-2021-26411漏洞攻击我国科研机构	芜琼洞	360政企安全
1月28日	提到涉及IE浏览器，但无法进一步分析	Lazarus	微软[38]
2月4日	韩国安全厂商ENKI发报告称朝鲜黑客攻击ENKI的研究人员	Lazarus	ENKI
3月9日	微软发布CVE-2021-26411漏洞公告	N/A	微软

• CVE-2021-26411漏洞关键披露信息

02.Exchange 0day漏洞攻击爆发，中国亦是受害者

今年3月，多个APT组织利用Exchange邮件服务器0day漏洞发起了攻击活动，安全公司ESET发布新的安全通告[39]：全球有115个国家地区超过5000台的Exchange服务器被攻破，10个不同的APT组织的攻击目标涉及亚洲，中东，美洲和欧洲地区的各国组织机构。

我们在3月3日发布了安全公告[40]，进一步监控发现从3月4日开始，中国地区的部分组织机构开始遭受Exchange漏洞的攻击。截至4月9日，至少有超过600台以上的中国地区Exchange服务器受到不同程度的攻击影响。

5.勒索攻击APT化，高级威胁技术、定向攻击手段层出不穷

2021年上半年，勒索病毒攻击问题也进入一个新的纪元，针对关键基础设施的攻击事件不断，开始呈现常态化迹象，有组织网络犯罪与国家级黑客组织的加入，使得一般机构面对勒索攻击无力招架，国家背景的Agrius使用带勒索功能的Apostle对以色列目标进行破坏[41]。根据Cybereason的报告显示，支付赎金的组织有八成会再次遭到攻击，大约半数为相同的攻击者。从DarkSide攻击美国石油管网到Conti入侵爱尔兰卫生部门，勒索病毒的攻击目标已经从个人电脑、服务器，到目前对医院、学校、政府机构和基础设施实施攻击，其影响力已经大大超越以往。这些勒索病毒攻击已与既往的国家级APT的攻击过程毫无差别，攻击过程APT化已经成为一个趋势。

上半年的勒索攻击事件，也再次印证了《2020年全球高级持续性威胁（APT)研究报告》中对2021年攻击趋势预测中，我们认为意图为破坏、窃密的针对性勒索攻击将不断出现。

• Colonial Pipeline公司紧急通告

01.勒索病毒威胁成为全球共同挑战，勒索威胁事关国家安全

在经历美国最大燃油管道运营商 Colonial Pipeline 遭黑客攻击以及网络犯罪分子造成的损害日益严重之后，美国司法部门正在将勒索软件攻击的调查提升到与恐怖主义类似的优先地位。而勒索病毒攻击问题，也不单单是某个国家或地区面对的挑战，其威胁已成为全球共同挑战。Conti入侵爱尔兰卫生部门，在刚刚结束不久的七国集团成员国峰会上，也发表联合声明，呼吁共同打击勒索软件攻击团伙。勒索病毒已不单单是造成经济上的损失，它已经形成了对国家安全，公众生命健康安全的挑战。未来我们面临勒索病毒的挑战将更加严峻，勒索病毒威胁的应对需提升到战略高度。

02.网络威胁超越传统安全威胁，关键基础设施成为黑客攻击目标

新冠病毒疫情对这个世界，对大众的生活、工作方式都产生了深远的影响。线上办公、远程会议、各类智能识别技术不断参与到社会运转之中。大数据驱动业务，整个世界构筑在软件之上。网络威胁对现实社会运转的影响力也切实凸显。政府机构、医疗卫生、教育、交通运输等大量基础公共服务面临勒索攻击的严峻挑战，安全威胁也正在超越传统安全威胁。

发布时间	攻击事件	涉及行业
1月21日	黑客利用Windows自带的BitLocker加密了法国Chwapi医院数据	医疗卫生
4月4日	荷兰最大物流服务供应商之一的Bakker Logistiek遭遇勒索病毒攻击	物流
5月7日	美国最大燃油运输管道商“科洛尼尔”(Colonial Pipeline) 公司遭遇勒索软件攻击	能源
5月10日	美国塔尔萨市遭受勒索软件攻击导致在线服务中断	公共服务
5月13日	爱尔兰卫生服务部门遭遇Conti勒索软件攻击	医疗卫生
6月2日	渡轮服务马萨诸塞州汽船管理局(Steamship Authority of Massachusetts)遭遇勒索攻击	交通

• 针对关键基础设施部分攻击活动

03.勒索危害加剧，信息泄露、双重勒索成主流

传统勒索主要以加密文件、数据库、磁盘等方式，影响信息系统正常运作，迫使受害者支付赎金。而从2019年11月开始Maze率先尝试通过泄密实施勒索，经过不到两年的发展，通过窃取数据进行的双重勒索已经成为主流，目前已有34个流行家族，例如Conti、Sodinokibi、DarkSide等都在以窃取和泄露数据作为胁迫筹码。这也更加剧了攻击的危害，勒索带来的信息泄露也跟加剧了企业的担忧。

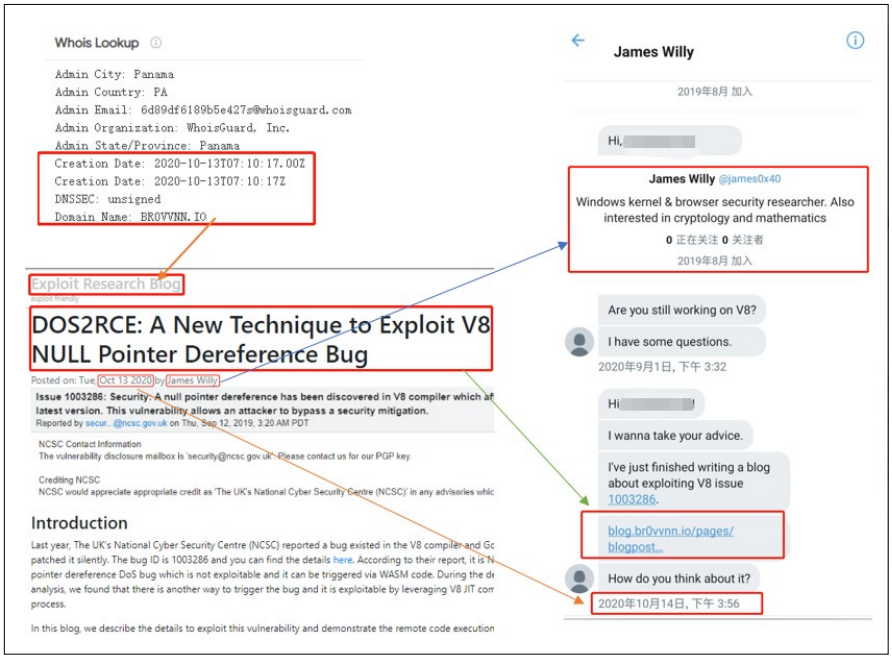
今年上半年，被曝光的事件中，超过8成是双重勒索情况，也就是针对规模较大的企业和机构的勒索攻击，双重勒索已经成为绝对的主流。4月，苹果的代工厂广达遭勒索病毒攻击，遭黑客团伙窃取大量资料，在勒索代工厂失败之后，黑客转而勒索苹果电脑公司高达5000万美元赎金，如果无法和攻击者达成协议，苹果将有大批数据泄露。

• Colonial Pipeline公司紧急通告

6.针对安全研究人员的社会工程学定向攻击

从去年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，到12月FireEye安全厂商在落鹰行动中被攻击，导致其红队安全工具被泄露。APT组织与安全机构之间的正面对抗不断升级，今年年初，google安全小组披露了一起利用推特等社交媒体针对安全研究人员的社会工程学攻击事件[42]。该事件将网络安全本质仍是人与人之间的对抗体现的淋漓尽致。

经过360高级威胁研究院的分析研判，结合360安全大脑的全网遥测分析，我们确认这是APT-C-26（Lazarus）组织首次针对网络安全行业并筹划了一年时间以上的APT攻击行动，此次行动该组织使用了针对数字加密货币和巨头商业公司等行业相似的攻击技战术，结合此次攻击中出现的有毒“POC”源码包等攻击技术特点，我们将此次攻击行动命名为“破壳行动”[43]。该组织建立BLOG、发布漏洞分析文章、伪装安全研究人员身份进行技术交流的完整细节过程，如下图所示：



- “破壳行动”攻击细节过程

角色	技术文章	时间
James Willy	DOS2RCE: A New Technique to Exploit V8 NULL Pointer Dereference Bug	2020年10月13日
Billy Brown and Zhanguo	Explicit Is Always Good? Read the Story of CVE-2020-1034	2020年10月18日
xixing	CVE-2020-1332 : Microsoft Excel Remote Code Execution Vulnerabiltity	2020年11月7日
James Willy	A Series of Windows Kernel Bugs in a Single Function	2021年1月15日
Zhang Guo	Exploiting CVE-2020-15994 Chrome WebAssembly Engine UAF Vulnerability	2021年1月20日

有毒“POC”源代码包在Visual Studio的工程配置文件中加入了恶意代码，如某个POC包dxgkrnl_poc.vcxproj工程配置文件，在PreBuildEvent字段中插入了一段命令。该命令会使用Powershell执行隐藏在本地工程中的DLL荷载，在工程编译时相关的恶意代码即会被触发执行。

总览整个攻击事件，APT-C-26 (Lazarus) 组织从提前一年注册社交账号开始策划攻击，到持续数月发布漏洞安全相关文章，推特、github、youtube等各大平台也持续发布相关资讯，引发大量安全博客、从业人员相继转载增加行业知名度，再到最终通过社工攻击针对安全研究人员发送带有恶意代码的POC源码包，可以说是一场非常有耐心且经过精心设计的攻击行动，不难猜测攻击者将安全从业人员作为目标，最终可能导致安全研究人员所属的安全公司被入侵渗透、重要安全漏洞研究成果被盗等严重危害。

• 该组织总共通过伪装的技术Blog发布了5篇漏洞分析文章。

PART 04

关键核心战场态势

1.政府、科研是重灾区，医疗、媒体威胁凸显

今年上半年，无论从国内受影响情况还是基于公开APT报告涉及行业统计，都可以看出政府、科研和国防军工依然是主要针对领域，其中针对我国教育领域的攻击活动实则是瞄准国防军工和科技创新体系。针对我国ICT供应商的供应链攻击威胁进一步升级，今年南亚、东南亚地区疫情形势严峻，5月初出现多起针对我国医疗卫生机构的攻击。涉及媒体领域重点单位的攻击频次较去年明显加强，且更具针对性。

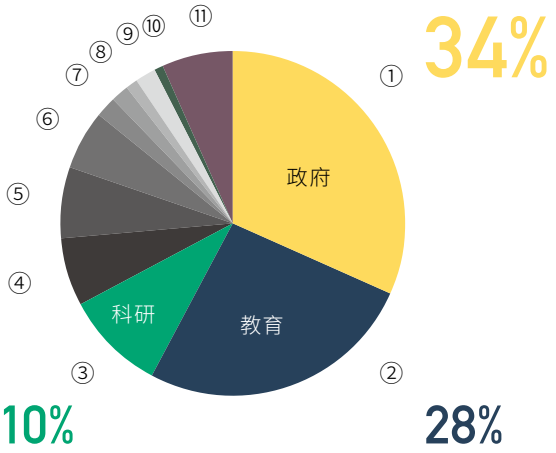


图1

①政府 34%
②教育 28%
③科研 10%
④国防军工 7%
⑤ICT供应商 6%
⑥贸易 2%
⑦制造 2%
⑧媒体 2%
⑨能源 1%
⑩医疗 1%
⑪其他 7%

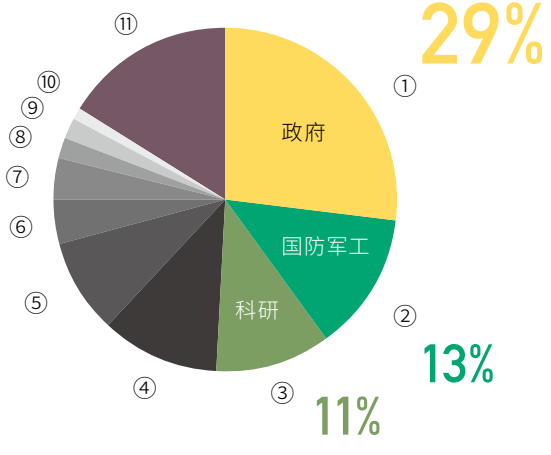


图2

①政府 29%
②国防军工 13%
③科研 11%
④能源 11%
⑤金融 9%
⑥医疗 4%
⑦教育 4%
⑧制造 2%
⑨航空 2%
⑩通信 1%
⑪其他 16%

• 图1.2021年上半年中国地区受影响行业分布 • 图2.2021年上半年公开APT报告涉及行业分布

2.城市数字化转型下APT威胁加剧

2021年3月11日，十三届全国人大四次会议表决通过了关于国民经济和社会发展第十四个五年规划和2035年远景目标纲要的决议。在国家十四五规划纲要中[44]，将“加快数字化发展，建设数字中国”单独成篇，从国家战略层面明确了数字化转型的重要性。2021年全国两会期间，全国政协委员，360集团创始人、董事长周鸿祎就智慧城市面临新型网络威胁，提出加快构建智慧城市安全基座的议案[45]。

从上半年APT攻击活动整体来看，行业领域是APT攻击首要关注因素，但由于地缘政治或其他因素导致的城市区域性攻击活动愈见明显，尤其随着城市数字化转型快速发展，APT攻击打法也会随之调整升级。

01.针对城市区域性的攻击威胁不断

针对我国的攻击活动中以朝鲜半岛、南亚等地区的APT组织最为显著，其中如Darkhotel、旺刺，以及今年新捕获的芜琼洞等组织，相关攻击活动都是以地域性特征为主，行业领域并不是其首要关注的。尤其是Darkhotel组织是长期围绕我国某地区，针对多个不同行业领域的单位或个人发起定向攻击。而南亚和东南亚组织攻击活动的地域性特性更多呈现周期性，尤其是在出现重大热点事件期间尤为明显。

APT化的定向勒索攻击针对市政公共设施和公共服务部门的攻击事件也层出不穷。今年4月末Babuk勒索病毒成功攻击美国华盛顿警方并窃取超250GB数据，在攻击者不接受支付赎金后，暗网公布了大量窃取的敏感数据。同月，巴西南里奥格兰德法院遭遇勒索病毒攻击[46]，员工资料、图片均无法正常使用。5月，美国塔尔萨市在线服务遭受勒索软件攻击[47]，导致在线支付系统、水费账单等服务中断，进一步塔尔萨市、塔尔萨市议会、塔尔萨警察局等网站也被关闭进行维护，严重影响到居民的正常生活。

无论是地缘政治背景下的APT攻击活动，还是暴利驱使下的勒索病毒威胁，在对城市安全造成重大挑战面前，急需围绕数据安全、网络安全，加快构建与城市数字化转型相适应的大安全格局。

02.万物互联下智慧城市的攻击面不断扩大

如今，智慧城市成为我国城市发展的新理念和新模式。据统计，我国已经有大约500座城市明确提出或正在建设新型智慧城市。然而，万物互联之下，以地理空间技术、物联网、互联网+、移动技术、大数据等技术做支撑的智慧城市建设，同样面临着不可估量的安全威胁。小到街道照明，大到能源、水务、电网、交通都与互联网连接，每个传感器都可能存在漏洞，加之专业级黑客组织的粉墨登场，智慧城市面临的网络安全威胁将越来越大。

国际调研机构IDC发布2021年中国智慧城市10大预测[48]：“到2023年，由于物联网生态系统的脆弱性，地方政府部署的设备中将有35%会成为恶意软件和勒索软件的攻击目标”。

APT组织也早已积极布局物联网战场，从去年Lazarus组织针对Aruba网络设备的攻击活动到今年针对路由器设备持续活跃的海莲花组织等。另外上半年我们监控发现了一系列围绕地理空间技术、5G等领域最新攻击活动。

• 暗网数泄露据网站公布华盛顿警方相关信息截图

3.ICT供应链攻击威胁进一步升级

2020年以供应商为核心目标的供应链攻击已趋于常态主流化，而今年上半年针对ICT (Information and Communication Technology，信息通信技术) 供应商的供应链攻击更是进一步增加，从供应设计研发到服务运维多个阶段都有涉及。海莲花组织更是将供应商攻击作为其主要攻击战术，2021年上半年的攻击活动中涉及多个头部软件供应商，较去年主要针对教育、政府以外，进一步涉及军工、科研等，而且主要针对供应商作业环境中的服务器设备。另外值得注意的是，去年年底蔓灵花组织积极探索的一种新型供应链攻击，今年已成常态主流。这类攻击目标并不是供应商和最终目标需求方，而是起到中介服务的招标代理机构。

01.倾向目标行业头部供应商

APT攻击活动的范畴主要取决于行业领域和具体单位目标，而针对某行业领域的攻击，实质上还是针对所属该行业的具体单位企业，只是目标更加广泛。而这些专注针对某一行业的ICT供应商，却间接起到中心化管理角色，也就是仅需针对该供应商攻击，其攻击收益是对应整个行业的目标单位，这也是导致APT青睐攻击这类供应商的原因。如海莲花针对高校领域的供应商就是这种情况。

02.优选目标单位强依赖供应商

在针对具体某单位的攻击中，APT组织会优先针对与该单位有密切合作的供应商，尤其是长期提供专属ICT服务的。由于供应商与服务单位之间紧密的合作关系，APT由此更容易接触目标单位核心业务等资源。比如去年魔鼠组织针对国内头部邮件系统服务提供商。

03.针对中介招标代理机构的攻击也需警惕

去年11月，我们捕获到蔓灵花组织针对供应链供应环节的一种新型攻击，这类攻击目标并不是供应商和最终目标需求方，而是起到中介服务的招标代理机构，这类机构起到企业和供应商之间的桥梁，虽然不提供具体产品或服务，但其能接触到完整的供需采购信息。

今年上半年该领域已成APT组织常态重点攻击目标范畴。我们发现被攻击的招标代理机构一般都有国资背景，其服务客户更多是国防军工、政府机构等重点单位。不难想象如果APT组织掌握了招标代理机构相关核心机密信息，那相应客户的完整供需关系即了如指掌。我们推测APT组织针对中介商的攻击意图，是其由此能获得更立体更全面的作战信息。

4.针对高等学校的攻击活动实则瞄准了我国国防军工和科技创新体系

今年上半年针对我国教育领域的攻击较去年又有进一步上升，近两年针对我们的攻击活动中，除政府机构以外，教育领域受影响最为严重，而其中高等学校是主要被攻击目标。高等院校是集聚高层次人才的战略高地，作为培养优秀人才的沃土、发展科研事业的基地，在建设世界科技强国的进程中，高校具有不可替代的作用。而APT组织针对高等学校的攻击活动，其实际意图是瞄准了我国的国防军工和科技创新体系，以窃取相关机密情报为最终目的。

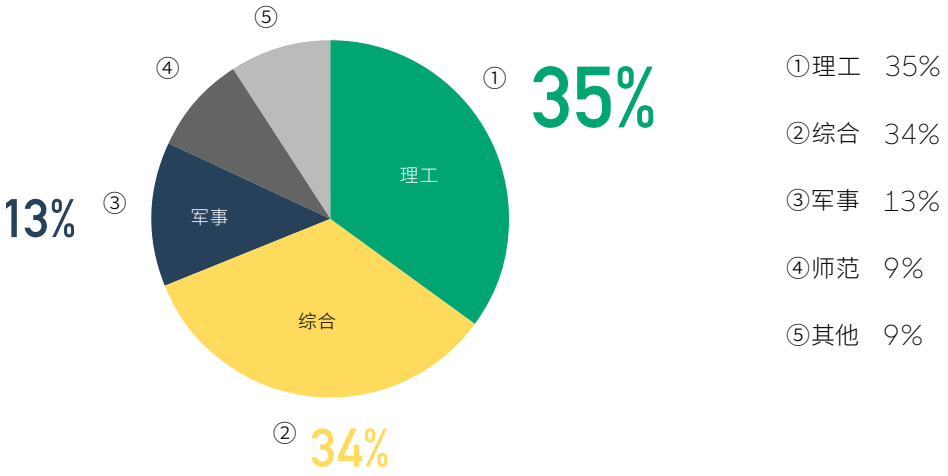
01.主要围绕科技创新相关

蔓灵花、毒云藤、海莲花等都是常年针对高等学校领域，大部分以钓鱼邮件为主，诱饵文档主要集中在科研相关通知、基金项目申请、高新科技等主题。个人所得税申报热点事件期间，毒云藤多次利用该事件主题制作诱饵文档向多家高校发起攻击。海莲花针对高校主要采用供应链攻击战术，瞄准的供应商均为教育行业头部企业。CNC组织在6月中旬我国航天相关时事热点前后，针对我国高等院校、科研机构相关航天领域进行情报窃取的定向攻击活动。

针对高等学校攻击活动中涉及科研相关部分诱饵文档
202105发布的3批XXX重点专项-含通知.pdf
2021年产学研合作基金项目信息表.xlsx
2021年度国家重点实验室开放课题申请指南.docx
2021年海洋试点国家实验室科技创新发展资金预算说明报告.docx
第六届XXX新材料大会通知.pdf
高超飞行器自适应动态规划的未来发展.docx
功能基元序构的高性能材料基础研究重大研究计划2021年度项目指南
国家遥感科技简报2020年第4期最新版.pdf
军工、国防装备配套需求信息发布平台.pdf
卫星遥感应用报告.pdf
叶企孙联合基金方向详细说明.pdf

02.国防军工背景高等学校是重点目标

基于去年和今年上半年被攻击的高等学校统计，我们发现理工和综合类院校共占整体7成，之后主要关注的是军事类院校。进一步我们深入分析发现被攻击的理工和综合类院校都有比较明显的共性，即相关院校大部分都涉及政府、国防等机构直属或共建直属或共建的情况。



• 被攻击高等学校类型占比

PART 05

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。下设APT技术分析、情报分析、引擎研发等6个核心部门，业务主要涵盖了高级威胁相关威胁鉴定、溯源扩线、监测预警、智能安全引擎、核心安全技术推导等多个关键领域。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组织的重要攻击行动，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。

参考链接

1.https://ti.dbappsecurity.com.cn/blog/index.php/2021/02/10/windows-kernel-zero-day-exploit-is-used-by-bitter-apt-in-targeted-attack/

2.https://mp.weixin.qq.com/s/dMFyLxsErYUZX7BQyBL9YQ

3.https://mp.weixin.qq.com/s/rMgQWQ8uW9foOy60LKtRJw

4.https://mp.weixin.qq.com/s/ELYDvdMiiy4FZ3KpmAddZQ

5.https://mp.weixin.qq.com/s/VTHvmRTeu3dw8HFyusKLqQ

6.https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34448

7.https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26411

8.https://enki.co.kr/blog/2021/02/04/ie_0day.html

9.https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/

10.https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_4.html

11.https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26411

12.https://blog.google/threat-analysis-group/update-campaign-targeting-security-researchers/

13.https://securelist.com/andariel-evolves-to-target-south-korea-with-ransomware/102811/

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

15.https://mp.weixin.qq.com/s/pkCK1ryXvGWFuoHQk9Rahg

16.https://mp.weixin.qq.com/s/bJrEwoq4QkDJvEk_ThvueQ

17.https://mp.weixin.qq.com/s/odBlrTBNXzJHDuXU_2IjZQ

18.https://www.volexity.com/blog/2021/05/27/suspected-apt29-operation-launches-election-fraud-themed-phishing-campaigns/

19.https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

20.https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf

21.https://unit42.paloaltonetworks.com/ironnetinjector/

22.https://mp.weixin.qq.com/s/odBlrTBNXzJHDuXU_2IjZQ

23.https://securityaffairs.co/wordpress/115360/apt/russia-apt-lithuanian-infrastructure.html

24.https://www.antiy.cn/research/notice&report/research_report/20210415.html

25.https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF

26.https://us-cert.cisa.gov/ncas/alerts/aa21-116a

27.https://www.fortinet.com/blog/threat-research/spearphishing-attack-uses-covid-21-lure-to-target-ukrainian-government

28.https://www.volexity.com/blog/2021/05/27/suspected-apt29-operation-launches-election-fraud-themed-phishing-campaigns/

29.https://ssu.gov.ua/novyny/sbu-zablokuvala-masovu-kiberataku-spetssluzhb-rf-na-kompiuterni-merezhi-ukrainskykh-orhaniv-vlady

30.https://msrc-blog.microsoft.com/2021/06/25/new-nobelium-activity/

31.https://www.bleepingcomputer.com/news/security/github-hosted-malware-calculates-cobalt-strike-payload-from-imgur-pic/

32.https://www.anomali.com/blog/probable-iranian-cyber-actors-static-kitten-conducting-cyberespionage-campaign-targeting-uae-and-kuwait-government-agencies

33.https://research.checkpoint.com/2021/irans-apt34-returns-with-an-updated-arsenal/

34.https://about.fb.com/news/2021/04/taking-action-against-hackers-in-palestine/

35.https://mp.weixin.qq.com/s/ELYDvdMiiy4FZ3KpmAddZQ

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

37.https://enki.co.kr/blog/2021/02/04/ie_0day.html

38.https://www.microsoft.com/security/blog/2021/01/28/zinc-attacks-against-security-researchers/

39.https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

40.https://mp.weixin.qq.com/s/4s66qdvVbUEzz-w9RcSUIg

41.https://assets.sentinelone.com/sentinellabs/evol-agrius

42.https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/

43.https://mp.weixin.qq.com/s/W-C_tKVnXco8C3ctgAjoNQ

44.http://www.gov.cn/xinwen/2021-03/13/content_5592681.htm

45.https://mp.weixin.qq.com/s/eLkgWowNvJR4qzKC8j1Jxg

46.https://www.bleepingcomputer.com/news/security/brazils-rio-grande-do-sul-court-system-hit-by-revil-ransomware/

47.https://www.bleepingcomputer.com/news/security/city-of-tulsas-online-services-disrupted-in-ransomware-incident/

48.https://www.idc.com/getdoc.jsp?containerId=prCHC47164720&utm_medium=rss_feed&utm_source=Alert&utm_campaign=rss_syndication

2021年/上半年
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