APT

全球高级持续性威胁 (APT)
2020年中报告

发布于 2020/06/29

奇安信 | 奇安信 威胁情报中心

前 言

奇安信威胁情报中心多年来持续跟踪分析全球高级持续性威胁（APT）活动趋势，总结高级持续性威胁背后的攻击组织在过去一段时间中的攻击活动和战术技术特点。

如今，2020年即将过去不平静的半年，而在全球网络安全领域也充满了变化和挑战。1月底，奇安信威胁情报中心监测到国外多个 APT 组织利用新冠疫情相关热点事件为诱饵对中国境内目标和机构实施 APT 攻击活动。随后利用新冠疫情实施的 APT 攻击活动被频频曝光。同时，由于企业远程办公和利用VPN远程接入企业网络的情况越来越普遍，多例围绕 VPN 应用的 APT 攻击活动也被发现。

本报告，总结了2020年上半年，全球范围内的主要APT活动情况，包括新的 APT 组织和地缘 APT 组织的活动变化趋势，以及上半年全球 APT 事件所呈现的趋势。

目 录

第一部分 上半年全球 APT 威胁态势

一、新冠疫情下的 APT 威胁活动

2020 年 1 月下旬开始，新冠肺炎疫情爆发。在此疫情形势下，APT 活动的活跃程度似乎并未受到影响，反而借用疫情热点事件内容为诱饵的攻击活动变得越发频繁。

根据奇安信红雨滴团队基于疫情相关网络攻击活动的监控来看，网络空间的攻击随着新冠病毒的扩撒而变化。

前期，从 2020 年 1 月下旬至 3 月初，相关网络攻击集中于针对汉语使用者，并多借以疫情相关中文热点诱饵信息进行攻击。相关诱饵包含的信息例如：“武汉旅行”、“申请登记”、”信息收集”、”卫生部”等等。

中后期，从 2 月中旬开始，以疫情信息为诱饵针对全球范围的网络攻击开始激增。诱饵信息开始转变为多种语言，以” Covid19”、”Covid”、”CORONA VIRUS”、”Coronavirus”、”COVID-19”等诱饵信息为主。

下图为红雨滴团队根据攻击活动相关的诱饵热词制作的词云图

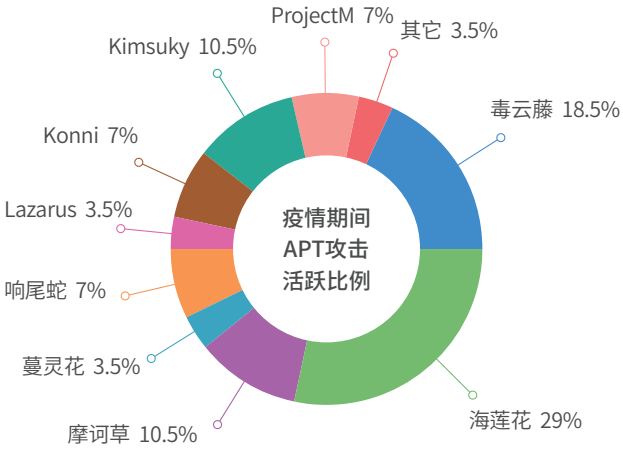
奇安信威胁情报中心持续跟踪着疫情相关攻击活动，2020年3月下旬，我们曾发布《COVID-19 | 新冠病毒笼罩下的全球疫情相关网络攻击分析报告》[6]一文，披露了2020年第一季度疫情相关攻击活动，之后，在红雨滴团队的持续监测过程中，我们又捕获了Lazarus、响尾蛇等组织利用疫情相关信息的攻击活动。

例如Lazarus组织利用疫情相关信息分发HWP恶意文档针对韩国的攻击活动。

我们整理了利用新冠疫情为诱饵内容的APT攻击组织和活动信息，包括如右图的APT 组织和活动。

活跃地域	APT组织和活动
东亚	Lazarus Group、Kimsuky、KONNI、毒云藤
东南亚	海莲花
南亚	摩诃草、蔓灵花、SideWinder、Transparent Tribe
东欧	Gamaredon Group
中东	Charming Kitten

根据奇安信威胁情报中心捕获的攻击样本等信息，我们在右图中列举了截止目前为止借疫情进行APT攻击的团伙活跃程度。



这些APT团伙主要攻击包括政府、军事、医疗等行业目标及相关人员，并且境外 APT 组织也积极利用疫情为诱饵针对我国目标实施 APT 攻击活动。

除了上述 APT 组织以外，网络犯罪团伙或威胁活动也利用疫情事件传播自身的恶意程序，其中包括Gorgon、TA505以及Packrat等。

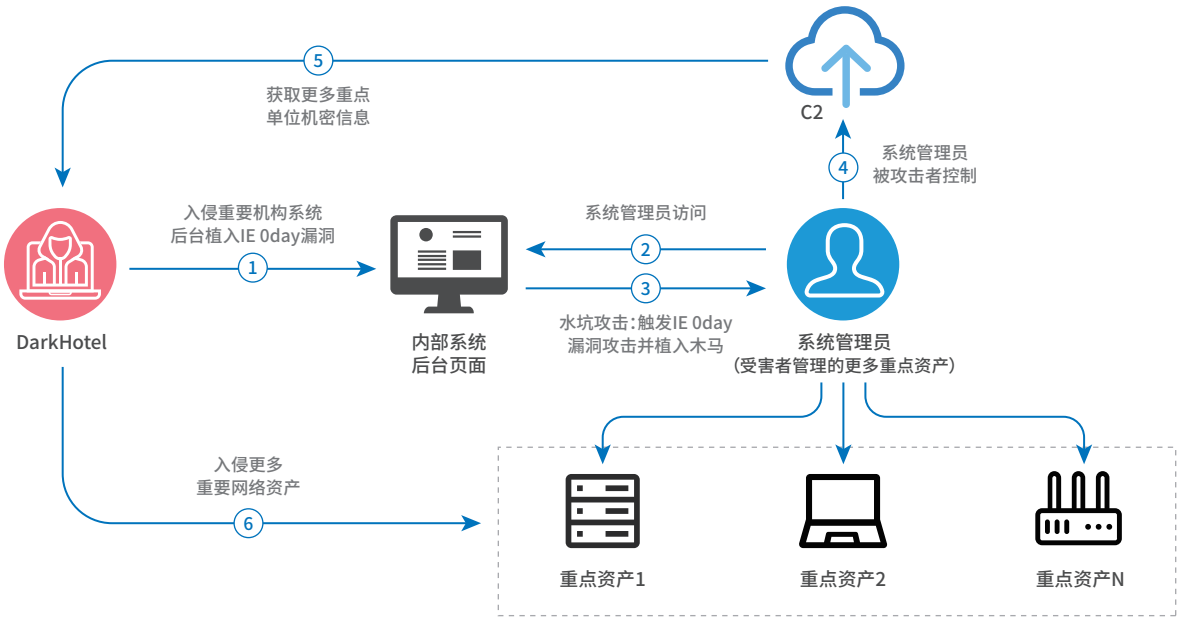
二、在野漏洞利用攻击的加剧

在2020年第一季度就被曝光和披露了多起在野漏洞利用的 APT 攻击活动：

- DarkHotel 使用两个针对浏览器的 0Day 漏洞（CVE-2019-17026、CVE-2020-0674）针对中国发起 APT 攻击；
- 国外安全厂商披露 Microsoft Exchange Control Panel (ECP) 漏洞 CVE-2020-0688 被在野利用；
- 火狐浏览器披露两个竞争条件导致的 UAF 漏洞 CVE-2020-6819 和 CVE-2020-6820 被在野利用；
- Chrome 浏览器漏洞 CVE-2020-6418 被在野利用；
- 某反病毒产品存在两个 0day 漏洞 CVE-2020-8467 和 CVE-2020-8468 被在野利用。

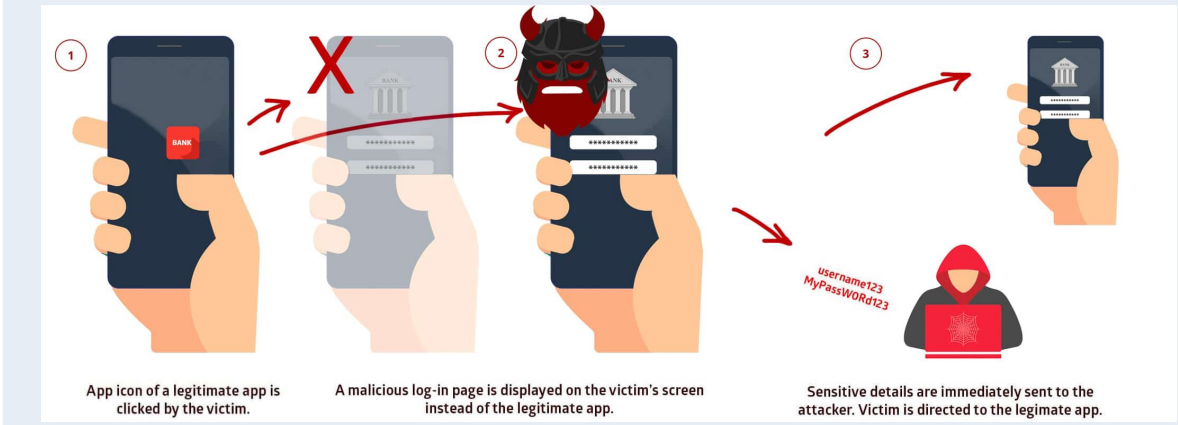
其中奇安信威胁情报中心捕获了DarkHotel利用CVE-2019-1367微软IE浏览器远程代码执行漏洞针对我国的定向攻击，由于相应利用代码在2019年 7月19日就被上传至受攻击服务器，而该漏洞微软在2019年9月份才修补，因此在攻击发生的当时漏洞还处于0day漏洞状态。所以可以推断，攻击者最晚在2019年7月就利用了该0day漏洞对我国实施网络攻击。

经过奇安信红雨滴团队对监控到的受害网络资产、攻击行为、恶意代码的详细分析和推理后认为：DarkHotel APT组织本次针对多个国内重要机构的内部系统管理页面植入IE 0day漏洞以执行水坑攻击，进而控制系统管理员的计算机以实施更广泛的入侵及横向移动。我们还原的整个攻击流程如下：



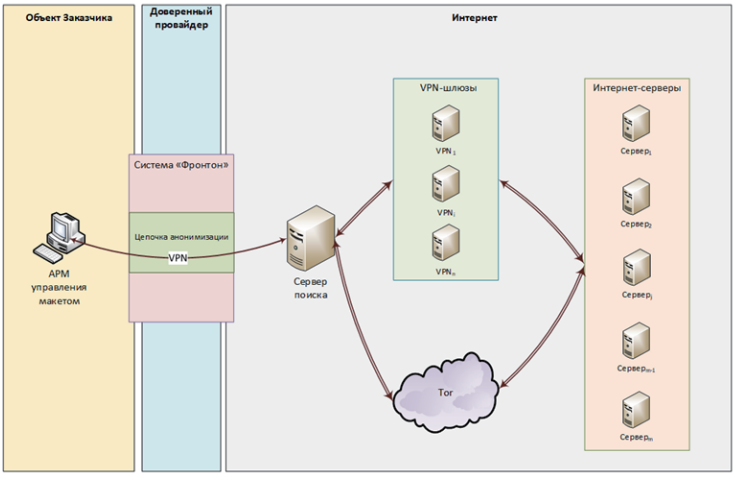
除了上述已经定性的APT攻击活动，还有一系列移动端已知漏洞也被各类国家级APT团伙用于定向攻击：

- 南亚次大陆地区的响尾蛇组织被发现利用 CVE-2019-2215 漏洞针对安卓终端目标用户实施移动端的 APT 攻击；
- iOS 邮件客户端爆出远程代码执行漏洞，已经被在野利用长达两年，漏洞不需要用户任何点击，只要给用户发送一封电子邮件，甚至邮件还在下载过程中，就能触发漏洞攻击，最后可达到获取 iPhone 数据的目的；
- 安卓特性漏洞 StrandHogg 2.0，与 StrandHogg 1.0 一样已经被攻击者在野利用。一旦在设备上安装利用了 StrandHogg 2.0 漏洞的 APP，受害者打开 APP 并输入凭证后，攻击者即可通过该恶意 APP 访问目标手机的短信消息和照片，并通过摄像头和录音监听目标。(如下图示意)



▲ 图引自：https://promon.co/strandhogg-2-0/

同时，在使用漏洞方面，不同国家级APT组织存在不同的利用漏洞的方式，而在2020年上半年，奇安信威胁情报中心独家披露了关于某国网络军火商，制作的一套IOT僵尸网络框架。

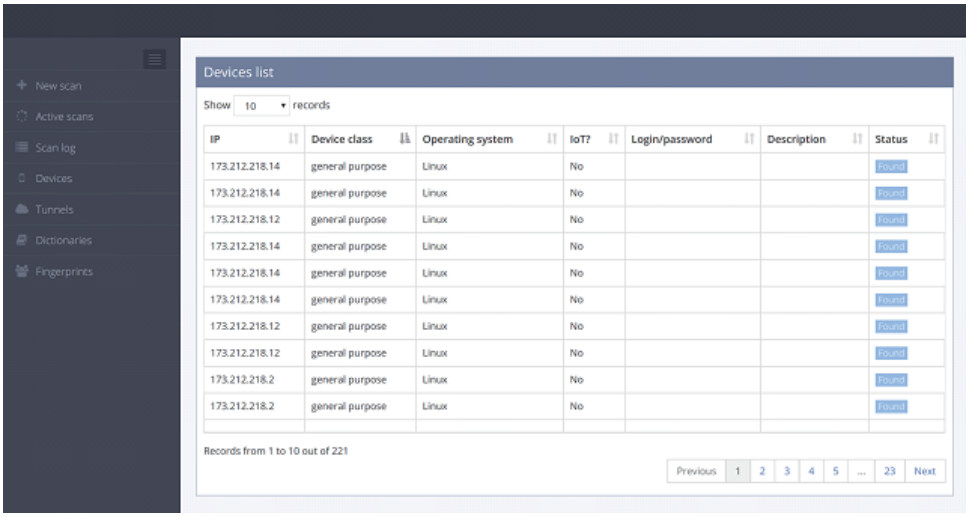


▲ 整个僵尸网络的网络拓扑图

右图为整个僵尸网络的网络拓扑图，该僵尸网络采用了通过VPN集群和Tor节点混合的流量回传机制，并将最终的数据回连到唯一一台用于接收所有数据的主机，该主机通过VPN接入最左侧的APM服务器环境，即 Apache+PHP+MySQL。

其主要相关模块如下：

- **暴力破解模块**
- **快速网络扫描模块:**
- **多平台载荷部署模块**



当然，除了这些表面的简单漏洞攻击之外，一些关于物联网的0day漏洞武器模块都会留有接口提供安装部署。参考此前的APT28组织构建的VPNFilter蠕虫型僵尸网络、北美地区情报机构通过入侵MikroTik RouterOS组建的僵尸网络，不难看出高维度网军均在IOT类僵尸网络中抢夺制高点，这对于在隐匿行踪与流量捕获方面都将是一个高级威胁趋势。

三、远程办公带来的新的 APT 威胁攻击面

新冠疫情在全球范围的蔓延，导致很多公司和机构采用了远程办公的方式，其通常依赖于 VPN 应用接入企业内部网络，这样也暴露了可用于攻击的重要攻击入口。从历史披露的 APT 活动来看，利用 VPN 或远程访问的脆弱性作为攻击入口一直较少被披露过。

上半年，有国外 APT 组织利用国内某知名安全公司VPN 的漏洞实现载荷的下发。除此以外，国外安全厂商披露的Fox Kitten组织就利用了多个 VPN 漏洞访问目标内网，其中包括针对Pulse Secure（CVE-2019-11510）、Fortinet FortiOS（CVE-2018-13379）、Palo Alto Networks VPN（CVE-2018-1579）。

此外，在疫情期间，DarkHotel和Wellmess组织分别利用我国厂商的VPN漏洞进行攻击，前者在这次行动主要针对基层单位，后者则主要针对中国多家高级别科研机构。当然，无论是手法还是攻击目标，均可见预谋已久。

第二部分 地缘背景下的 APT 组织和活动

从上半年的全球 APT 组织和活动披露来看，APT 威胁的整体活跃水平还是保持了一个比较高的频度，主要活跃的 APT 组织还是过去熟知的，中东地区依然是 APT 活动最为频繁和错综复杂的地域，活跃着数量众多的 APT 组织。

在上半年的公开 APT 类情报中，出现了 4 个新命名的 APT 组织和活动，并且主要活跃于中东地区。

1.WildPressure

WildPressure 是卡巴披露的一个恶意攻击活动 [1]，该活动最早于 2019 年 8 月被发现，其分发了一个成熟的 C ++ 木马，并且所有的木马文件的编译时间戳都是相同的，均为 2019 年 3 月。唯一实现的加密是针对不同受害者具有不同 64 字节密钥的 RC4 算法。该活动主要针对中东地区的工业相关实体。

2. 诺崇狮

诺崇狮是由奇安信威胁情报中心新发现并命名的一个 APT 组织 [2]，该组织活跃在中东地区，其最早的样本文件可以追溯到 2013 年 9 月，在其历史活动中通常利用社交网络（如 Twitter，Telegram，youtube 等）进行非定向的水坑传播式钓鱼攻击及定向目标的鱼叉攻击，并主要针对移动终端实施攻击。

▲ 诺崇狮（APT组织）

2013.09.18
首个攻击样本出现。

2015.04.22
在也门干预行动阶段“Operation Restoring Hope”首天，于 Twitter 社交平台上陆续发起多个水坑和鱼叉攻击。钓鱼攻击中至少有四名。

2017.09.17
持续在 Youtube 媒体平台上，进行先后五次的水坑攻击，合计有万名用户看到钓鱼信息。钓鱼攻击者至少有两名。

2017.09.25
一名钓鱼攻击者在 Qassimy 游戏网站发布钓鱼游戏信息，进行水坑攻击。

2018.01.15
一名钓鱼攻击者在 Gem-Flash 网站发布钓鱼游戏信息，进行水坑攻击。

2018.06.20
钓鱼攻击者在 Telegram 聊天平台上创建 2018 世界杯直播相关的钓鱼频道“cups2018”，进行水坑攻击。

2018.08.02
一名钓鱼攻击者在 ADSGASTE 数字门户网站发布世界比直播的钓鱼信息，进行水坑攻击。

3.Fox Kitten

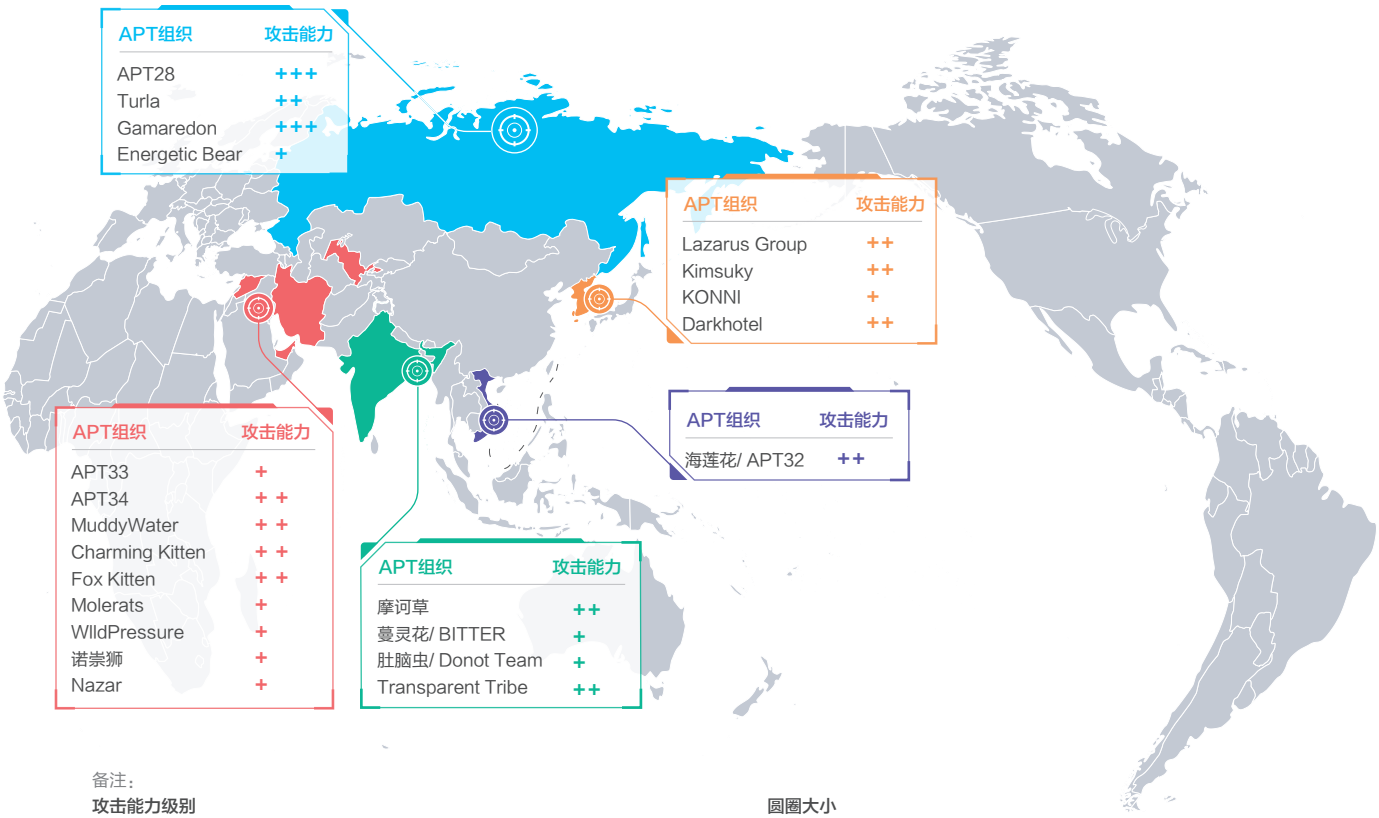
Fox Kitten 是由国外安全厂商 ClearSky 发现并命名的中东地区APT 组织[3]。ClearSky在2019年第四季度发现其持续三年的攻击活动，该团伙可能和 APT33和 APT34相关，并且也确定了 APT33和APT39之间的联系。

相关活动是通过使用各种攻击性工具进行的，其中大多数是基于开放的源代码，而有些是自行开发的。其还利用了 RDP 和 VPN 的漏洞。

4.Nazar

Nazar 是国外安全研究人员在OPCDE 会议上公开披露和命名的 APT 活动[4]，其是对ShadowBrokers 泄露资料中，TeDi签名为SIG37的 APT 组织的归属。而 TeDi 签名是某西方大国情报机构对全球其他 APT 组织和活动的跟踪项目，并且以 sigXX 的形式代号进行命名。CrySyS实验室在此前对 TeDi 签名 SIG37归因为IronTiger，而此次安全研究人员对其发表了不同的结论，其实际攻击活动可能和中东地区有关，并且最早可以追溯到2008年，并集中在2010-2013年。

在此报告中，我们依旧按 APT 组织主要活动的地域分布对其进行分析和跟踪，2020年上半年全球主要活跃的 APT 组织和活动地域分布如下图所示。



备注：

攻击能力级别

+++ 具备相当复杂的自定义攻击框架和丰富0day漏洞攻击资源。

++ 具备成熟的自制攻击载荷，漏洞利用和攻击技术，攻击活跃。

+ 具备攻击武器的组合使用和定制能力，缺乏完备的自制攻击工具或攻击不活跃。

圆圈大小

代表地缘性APT组织近年来活跃频度，主要根据公开披露事件和攻击活动。

图例

疑似地域归属 未知地域归属

东亚
East Asia

2020 年上半年前期东亚地区的 APT 组织主要以 Kimsuky 和 KONNI 的 APT 活动为主，其主要攻击包括韩国在内的目标。相关攻击活动继续以鱼叉邮件投递诱饵文档为主，其也积极利用新冠疫情作为热点事件分发攻击诱饵。在 4 月中旬之后，东亚地区的老牌 APT 组织 Lazarus 开始发起攻击活动，并利用波音等国际大公司招聘信息为诱饵开展了多次攻击。

在过去我们也曾总结过 Kimsuky 组织主要以政治动机为目的，重点针对韩国目标的攻击活动，这里我们总结上半年的部分攻击活动如下：

- 针对韩国居民教育官员的鱼叉邮件攻击，使用的诱饵为 PDF 文件；
- 利用新冠肺炎疫情为诱饵内容实施鱼叉邮件攻击；
- 利用伪装成 HWP 简历文档的 scr 文件实施攻击；
- 以美国国务卿为诱饵内容的攻击文件；
- 伪装成韩国第二十一届国民议会选举文件的攻击活动。

KONNI 组织归属的公开判定一直没有非常明确的定论，奇安信威胁情报中心结合过去的跟踪研究，认为其是东亚某地区语系的 APT 组织，其曾在2019年7月至2019年10月之间针对美国政府实施鱼叉邮件攻击，并且在今年1月中旬制作了带有“**中央委员会”和“东京残奥会”等相关诱饵信息的诱饵文件。之后在5月下旬，该组织以核安全等敏感话题开展了多次的攻击活动。

Lazarus Group 被认为是东亚某国政府背景的最为古老也是最为活跃的 APT 组织之一，在 2 月份，美国 US-CERT 再次披露了一批 Lazarus Group 相关的攻击武器库资料 [5]，其中涉及 7 个木马家族。Lazarus 使用的新的攻击木马描述信息如下：

攻击工具名称	功能说明
BISTROMATH	一款全功能 RAT
HOPLIGHT	木马，使用公共SSL证书进行安全通信
SLICKSHOES	通常作为Loader 或者 Dropper 程序
CROWDEDFLOUNDER	内存驻留 RAT
HOTCROISSANT	植入程序，网络流量利用 XOR 加密
ARTFULPIE	通过获取和注入DLL 载荷
BUFFETLINE	植入程序，使用RC4编码和PolarSSL混淆网络通信

从上述新的攻击工具功能说明也可以看出，Lazarus Group 一直在频繁开发和更新其攻击工具集。之后自四月初开始，Lazarus Group 开展了多次攻击活动，使用了以波音公司、军舰企业等敏感企业招聘信息的诱饵文档。

▲ 以波音，军舰相关为诱饵的样本内容

DarkHotel 是东亚地区另一个活跃的 APT 组织，其擅长于利用 0day 和 1day 漏洞实施攻击。该组织上半年多次被监测到针对我国境内目标实施攻击，其中主要包括利用了两个浏览器 0day 漏洞（CVE-2020-0674，CVE-2019-17026）针对我国政府机构实施 APT 攻击，以及利用国内某知名安全公司 VPN 漏洞针对境内多个机构实施 APT 攻击活动。

安全厂商 ESET 近日又披露了该组织新恶意框架 Ramsay，Ramsay 框架是疑似专门用于针对隔离网络的恶意代码，主要通过感染正常软件进行传播，同时与常规恶意软件基于网络协议的 C2 不同，Ramsay 框架采用的是自定义的文件传输控制指令，当扫描到被带入隔离网络的感染文件，则从文件特定位置读取指令执行。

东南亚
Southeast Asia

海莲花组织是东南亚地区最为活跃的 APT 组织。在上半年新冠肺炎疫情爆发期间，海莲花组织同时利用了“新冠病毒疫情”和“禽流感疫情”的热点事件作为诱饵攻击我国政府和相关科研实验室机构。

▲ 海莲花组织利用疫情作为诱饵

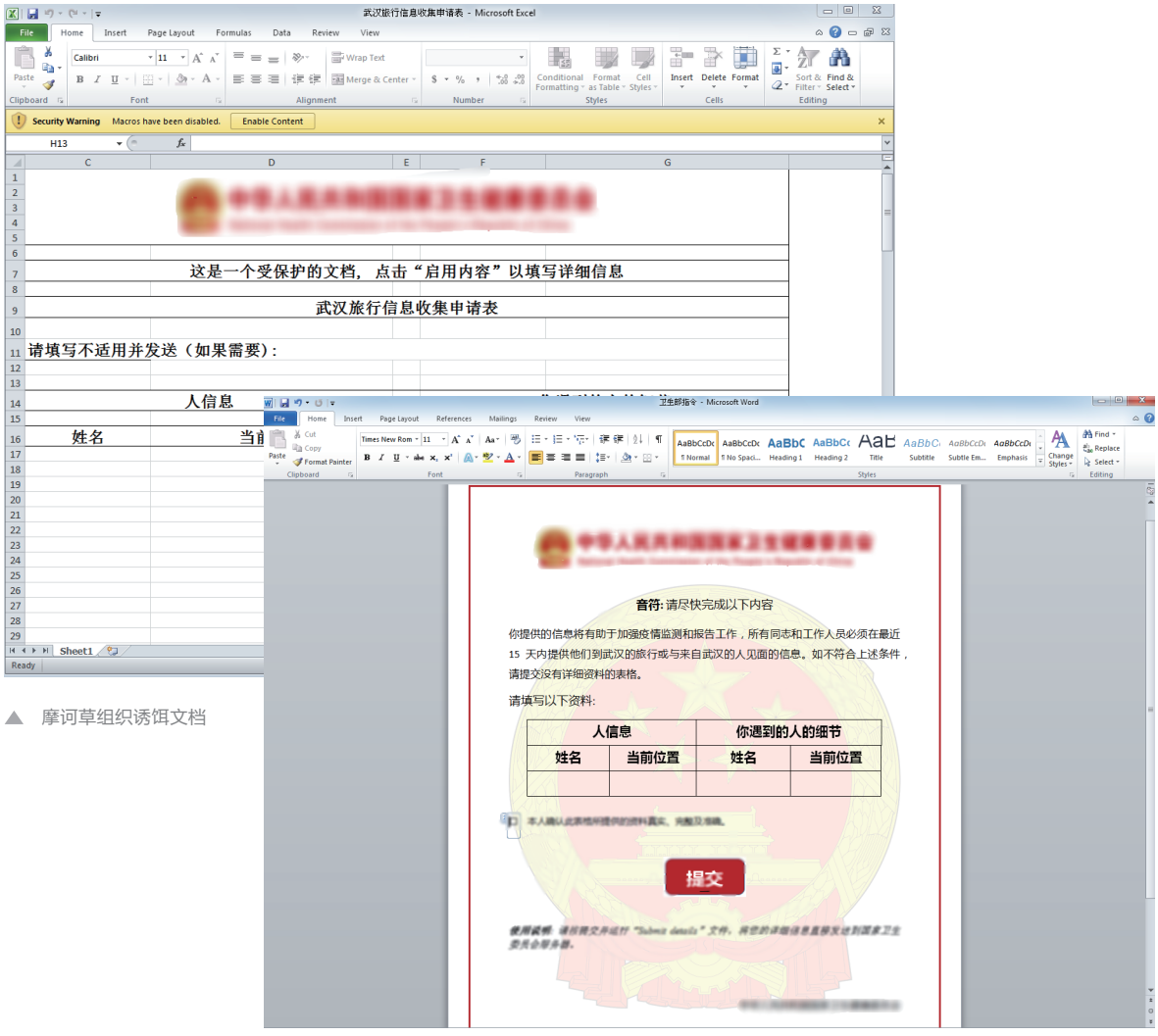
而其依旧延续了过去的攻击战术和技术手段，其中通过利用 WPS 文字处理软件的白利用方式加载恶意 DLL 文件，并用于最终加载执行海莲花特有的 Denis 木马。

南亚次大陆
South Asian subcontinent

在过去的 APT 威胁分析报告中，我们也多次提及南亚地区活跃的多个 APT 组织，包括摩诃草、蔓灵花、肚脑虫等，并且这些 APT 组织过去无论在攻击目标上，还是在攻击工具特征上都存在一些关联性和重叠。除了这些 APT 组织外，国内其他友商命名的“响尾蛇” APT 组织也活跃在南亚地区，奇安信威胁情报中心在过去的跟踪中也找到了响尾蛇组织和摩诃草的一些强关联性证据，所以在内部将其合并跟踪。

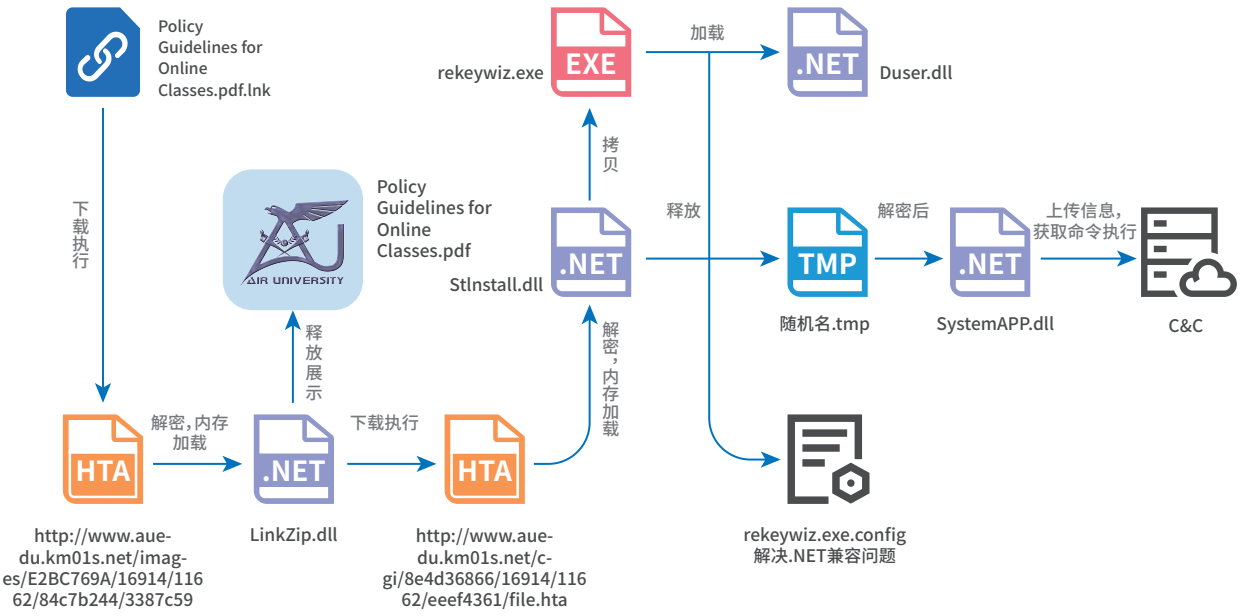
在 2020 年上半年的 APT 攻击活动中，我们都有发现摩诃草、蔓灵花组织利用新冠疫情事件对国内目标实施的 APT 攻击活动。在疫情爆发初期，摩诃草组织便利用“** 旅行信息收集申请表 .xlsm”，“卫生部指令 .docx”等诱饵对我国进行攻击活动，并且该组织也是第一个被披露利用疫情进行攻击的 APT 组织。

下图展示了部分诱饵文档的内容：



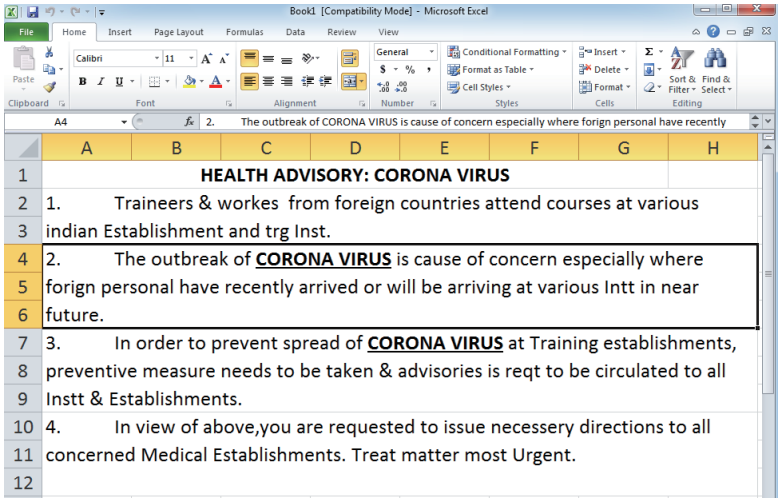
▲ 摩诃草组织诱饵文档

同时与摩诃草存在重叠的响尾蛇 APT 组织也开始利用“** 疫情处理方法”、“** 大学疫情期间网络课程”等新冠相关诱饵信息开展了针对巴基斯坦的攻击活动：



南亚次大陆地区还活跃着另一个名为 Transparent Tribe 的威胁组织，其通常又被命名为 APT36、ProjectM、Operation C-Major，从奇安信过去针对该组织活动的追溯来看，其成员可能活跃在南亚次大陆地区。该组织不具备特别复杂的攻击形式和攻击工具，并且从过去的活动来看，其同时实施以网络间谍为目的的 APT 活动和牟利为目的的网络犯罪活动。

奇安信威胁情报中心在上半年也监测到该组织构造了一个与南亚某国电子信息处高度相似的域名 hxxp://email.gov.in.maildrive.email/ 进行恶意样本下发。获取到的样本为宏利用文档，并通过文档内容诱使受害者启用宏，最终展示新冠病毒相关信息。



	A	B	C	D	E	F	G	H
1	HEALTH ADVISORY: CORONA VIRUS							
2	1. Traineers & workes from foreign countries attend courses at various							
3	indian Establishment and trg Inst.							
4	2. The outbreak of CORONA VIRUS is cause of concern especially where							
5	forign personal have recently arrived or will be arriving at various Intt in near							
6	future.							
7	3. In order to prevent spread of CORONA VIRUS at Training establishments,							
8	preventive measure needs to be taken & advisories is reqt to be circulated to all							
9	Instt & Establishments.							
10	4. In view of above,you are requested to issue necessery directions to all							
11	concerned Medical Establishments. Treat matter most Urgent.							
12								

其最终释放的木马为该组织独有的远控木马 Crimson RAT。具有远程 Shell、上传、下载文件、获取进程信息、结束指定进程等多种远控功能。

东欧
Eastern Europe

从公开披露来看，东欧地区的 APT 组织在上半年的攻击活动并没有出现显著变化，像 APT28、Turla、Gamaredon group 和 Energetic Bear 组织都有部分活动，其中包括：

- APT28 针对乌克兰能源公司 Burisma Holdings 及其子公司和合作伙伴的员工的电子邮件凭据窃取；
- 国外安全厂商披露自 2019 年 5 月以来，APT28 组织就一直在滥用受感染的电子邮件地址来发送凭据网络钓鱼垃圾邮件；
- Gamaredon 从 2019 年 12 月起针对乌克兰安全机构的攻击活动；
- 亚美尼亚几个网站被披露在 2019 年初被 Turla 实施水坑攻击，植入 js 并分发恶意 Flash 更新，利用 evercookie 跟踪用户，并且使用 .Net 和 Python 开发的载荷，这是 Turla 首次使用 python 开发攻击载荷；
- 4 月份，Energetic Bear 组织对旧金山两个机场实施了 APT 攻击活动；
- Turla 组织利用 COMRAT 新版本针对多个欧洲国家会议与外交部的攻击活动。

其中最为典型的事件案例还是奥地利政府针对 Turla 组织在一月份针对其国务院网络的攻击事件的响应和防御，奥地利政府最终成功防御相关攻击活动，并破解了 Turla 投递载荷的加密通信方式。

中东
Middle East

从 2020 年伊始，鉴于中东地区发生的政治军事冲突事件，国外安全厂商纷纷发布中东地区 APT 组织的历史总结报告，并预警未来可能发生的 APT 攻击活动。但从上半年的披露来看，中东地区 APT 组织并未因此事件而引发针对美国政府实施大规模的网络攻击反击行为。

不过国外安全厂商也披露了中东地区 APT 组织的一些攻击武器的变化和攻击活动，例如：

- APT34 使用的新的基于 PowerShell 的攻击程序 PowDesk，其用于针对目标是运行 LANDesk Management Agent 的主机；
- APT34 针对美国公司 Westat 的攻击活动，并使用了更新的工具；
- APT34 可能入侵了属于黎巴嫩政府实体的 Microsoft Exchange Server，并更新了 Karkoff 载荷；
- 国外安全厂商披露 APT33 联合 Parisite 组织利用 Password-Spraying 技术攻击美国电力公司，而 Parisite 组织曾与攻击巴林石油公司事件有关；
- APT33 至少从 2019 年 11 月下旬至 1 月 5 日期间针对欧洲能源部门的攻击活动，并且被安全厂商发现与欧洲能源部门组织的邮件服务器通信的 PupyRAT 命令和控制（C2）服务器；
- APT33 开发的新的 .Net 载荷程序，国外安全厂商将其命名为 POWERBAND，其是之前 POWERTON 工具的变种；
- 在 2019 年中至 2020 年 1 月中之间，MuddyWater 进行的一系列鱼叉运动，并针对土耳其，约旦，伊拉克的政府组织，以及格鲁吉亚和阿塞拜疆的全球政府间组织和未知实体；
- 安全研究人员在 RSA 大会上披露 MuddyWater 组织使用鱼叉邮件分发 ForeLord，并实施了在 2019 年中期至 2020 年 1 月中旬的 APT 活动，其中 ForeLord 是一个窃取凭据的工具；
- Chafer APT 组织使用公开黑客工具针对科威特，沙特阿拉伯航空，政府部门的攻击活动；
- Greenbug 针对南亚电信行业的攻击活动。

从上述的攻击活动来看，中东地区具有政府背景的 APT 组织在攻击动机和目标选择上还是存在一些划分。APT34 和 MuddyWater 主要针对政府相关实体实施 APT 攻击，APT33 更倾向针对能源、电力行业等目标。

从战术技术上来看，鱼叉攻击是其主要的攻击入口，在攻击工具上更倾向于使用 PowerShell 和 .Net 开发的程序，而另一个 Charming Kitten 组织则更偏好于利用钓鱼网站实施攻击。

总 结

从 2020 年上半年来看，尽管新冠疫情在全球呈现爆发趋势，但是 APT 组织的攻击活动并没有停止。从公开披露的信息来看，APT 攻击的入口不再只重点围绕鱼叉邮件攻击和定向的凭据钓鱼，利用 0day 或者 Nday 漏洞实施攻击显得更加高效，包括利用一些远程服务、VPN，或者针对目标网络基础设施的漏洞，包括 Microsoft Exchange，Citrix 相关产品等。

结合疫情下的远程办公的趋势，这种改变，可能会给 APT 组织未来采用的攻击入口和战术方式带来一些变化。从防护角度上来看，防御 APT 攻击不仅需要做好人员安全意识教育，邮件和终端安全检测等防御手段外，还需要考虑到远程接入和关键网络基础设施的安全防护和监测能力。

2020 年下半年，针对我国的 APT 攻击频次也许会减少，但是精度会提升一个量级，这从各国国家级 APT 组织网络武器能力的提升，以及 0day 武器的运用情况可见一斑。因此针对 APT 攻击的防御更需要我们开展全面的体系化网络安全建设，一起构筑对抗高级持续性威胁的网络安全防线。

附录 1 奇安信威胁情报中心

奇安信威胁情报中心是北京奇安信科技有限公司（奇安信集团）旗下的威胁情报整合专业机构。该中心以业界领先的安全大数据资源为基础，基于奇安信长期积累的核心安全技术，依托亚太地区顶级的安全人才团队，通过强大的大数据能力，实现全网威胁情报的即时、全面、深入的整合与分析，为企业和机构提供安全管理与防护的网络威胁预警与情报。

奇安信威胁情报中心对外服务平台网址为https://ti.qianxin.com/。服务平台以海量多维度网络空间安全数据为基础，为安全分析人员及各类企业用户提供基础数据的查询，攻击线索拓展，事件背景研判，攻击组织解析，研究报告下载等多种维度的威胁情报数据与威胁情报服务。

▼ 奇安信威胁情报中心对外服务平台

微信公众号
奇安信威胁情报中心

微信公众号
奇安信病毒响应中心

附录 2 红雨滴团队（RedDrip Team）

奇安信旗下的高级威胁研究团队红雨滴（天眼实验室），成立于2015年，持续运营奇安信威胁情报中心至今，专注于APT攻击类高级威胁的研究，是国内首个发布并命名“海莲花”（APT-C-00，OceanLotus）APT攻击团伙的安全研究团队，也是当前奇安信威胁情报中心的主力威胁分析技术支持团队。

目前，红雨滴团队拥有数十人的专业分析师和相应的数据运营和平台开发人员，覆盖威胁情报运营的各个环节：公开情报收集、自有数据处理、恶意代码分析、网络流量解析、线索发现挖掘拓展、追踪溯源，实现安全事件分析的全流程运营。团队对外输出机读威胁情报数据支持奇安信自有和第三方的检测类安全产品，实现高效的威胁发现、损失评估及处置建议提供，同时也为公众和监管方输出事件和团伙层面的全面高级威胁分析报告。

依托全球领先的安全大数据能力、多维度多来源的安全数据和专业分析师的丰富经验，红雨滴团队自2015年持续发现多个包括海莲花在内的APT团伙在中国境内的长期活动，并发布国内首个团伙层面的APT事件揭露报告，开创了国内APT攻击类高级威胁体系化揭露的先河，已经成为国家级网络攻防的焦点。

奇安信红雨滴团队

关注微信公众号

附录 参考链接

1. https://securelist.com/wildpressure-targets-industrial-in-the-middle-east/96360/
2. https://ti.qianxin.com/blog/articles/who-is-the-next-silent-lamb-nuo-chong-lions-apt-organization-revealed/
3. https://www.clearskysec.com/fox-kitten/
4. https://www.epicturla.com/blog/the-lost-nazar
5. https://www.us-cert.gov/northkorea
6. https://ti.qianxin.com/blog/articles/coronavirus-analysis-of-global-outbreak-related-cyber-attacks/