APT

全球高级持续性威胁 (APT)
2020年度报告

2021年01月

奇安信 威胁情报中心 | 奇安信

奇安信 威胁情报中心 | 奇安信

邮箱：ti_support@qianxin.com
电话：4009-303-120
官网：https://ti.qianxin.com
扫描关注我们的微信公众号

主要观点

◆ 医疗卫生行业史上首次超过政府、金融、国防、能源、电信等领域，成为全球 APT 活动关注的首要目标。全球 23.7% 的 APT 活动事件与医疗卫生行业相关。针对疾控与防疫机构、病毒研究机构、疫苗研发机构和其他相关的医学研究机构的高级威胁活动持续不断。

◆ 中国首次超过美国、韩国、中东等国家和地区，成为全球 APT 活动的首要地区性目标。面对世界百年未有之大变局，中国的经济与科技发展，正在经受着前所未有的巨大考验。针对中国领先的科研机构、科技企业的网络窃密活动与网络破坏活动持续加剧。

◆ 2020 年，全球 APT 活动呈现出三大特点：疫情热点信息成 APT 活动常用诱饵，供应链和远程办公成为攻击切入点，定向勒索威胁成为 APT 活动新趋势。

◆ 网络安全、互联网、芯片与半导体等行业成为 2020 年 APT 活动关注的新兴热点，出现了很多新的攻击特点，发生了多起影响深远的 APT 攻击事件。

◆ 0day 在野利用在 2020 年持续高发。攻击者选用的漏洞目标逐渐从 Windows 下的原生浏览器，向 Chrome、Firefox 等用户量更大的浏览器转移，如果用一句话来总结 2020 年的 0day 在野利用情况，我们愿称之为“Chrome 漏洞利用年”。

◆ 我们预测，在 2021 年，APT 活动将呈现出如下六个趋势：疫苗及相关产业将会遭到持续攻击；针对中国的 APT 行动将持续加剧；远程办公的各个环节都将遭受 APT 攻击；地区冲突将引爆更激烈的网络战；网络武器库的泄露或将常态化；APT 组织可能组建基于 5G 与 IPv6 技术的物联网僵尸网络

摘 要

◆ 2020 年，奇安信威胁情报中心收录了高级威胁类公开报告共 642 篇，涉及了 151 个命名的攻击组织或攻击行动，其中，提及率最高的五个 APT 组织分别是：Lazarus：10.3%，Kimsuky：7.8%，海莲花：5.4%，Darkhotel：4.8%，蔓灵花：3.2%。

◆ 本次报告对开源情报中高级威胁活动涉及目标的国家和地域分布情况进行了分析和整理，监测显示高级威胁攻击活动几乎覆盖了全球绝大部分国家和地区。其中，开源情报中提及率最高的五个受害国家分别为：中国占比 7.4%，韩国：6.6%，美国：4.9%，巴基斯坦：3.2%，印度：3.2%。

◆ 中国首次超过美国、韩国、中东等国家和地区，成为全球 APT 攻击的首要地区性目标。

◆ 医疗卫生行业史上首次超过政府、金融、国防、能源、电信等领域，成为全球 APT 活动关注的首要目标。

◆ 2020 年，疫情热点信息成 APT 活动常用诱饵；供应链和远程办公成为切入点；定向勒索威胁成为 APT 活动新趋势

◆ 海莲花组织依旧是东南亚地区最为活跃的 APT 组织。

关键字：全球高级持续性威胁、APT、攻击组织、行动报告、定向攻击、网络犯罪

目 录

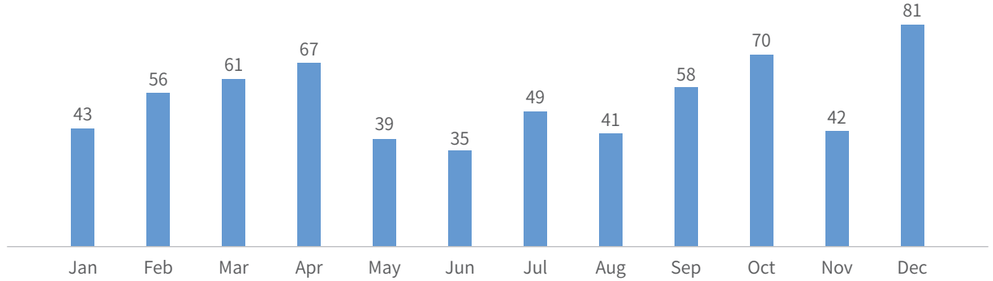
第一章 全球高级持续性威胁综述

公开来源的 APT 情报（以下简称“开源情报”）分析是了解全球网络安全研究机构安全关注，认知全球高级持续性威胁发展趋势的重要手段之一。2020 年，奇安信威胁情报中心对全球 200 多个主要的 APT 类情报来源进行了持续监测，监测内容包括但不限于 APT 攻击组织报告、APT 攻击行动报告、疑似 APT 的定向攻击事件、APT 攻击相关的恶意代码和漏洞分析，以及我们认为需要关注的网络犯罪组织及其相关活动。但由于来源众多，监测可能有所遗漏，敬请谅解。

本章内容及结论主要基于对上述开源情报以及内部威胁雷达数据的整理与分析。

一、全球高级威胁研究情况

奇安信威胁情报中心在 2020 年监测到的高级持续性威胁相关公开报告总共 642 篇。各月监测数据如下图所示。

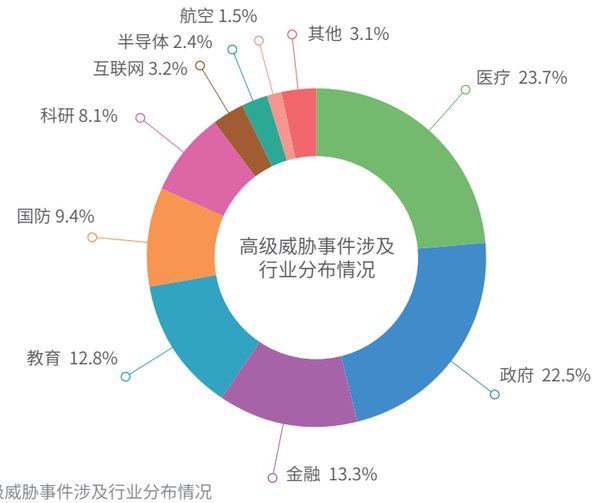


▲ 图 1.1 2020 年全球每月公开的威胁报告数量统计

二、受害目标的行业与地域

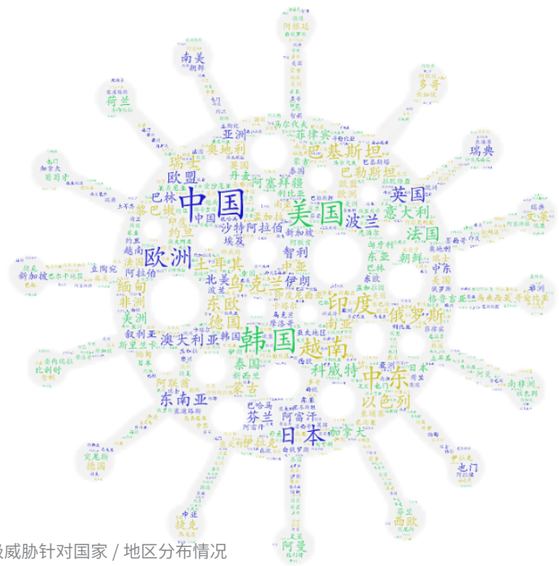
2020 年，新冠疫情席卷全球，从而带来新的网络攻击变化。通过开源情报并结合奇安信威胁情报中心威胁雷达数据显示：在全球 2020 年披露的 APT 相关活动报告中，涉及医疗卫生行业的事件占比为 23.7%，其次是政府（包括外交、政党、选举相关）22.5%，金融（包括银行、证券、数字货币等）、教育和国防（包括军事、军工、国防相关）紧随其后。这也是医疗卫生行业史上首次超过政府、金融、国防、能源、电信等领域，成为全球 APT 活动关注的首要目标。

2020 年高级威胁事件涉及行业分布情况



▲ 图 1.2 2020 年高级威胁事件涉及行业分布情况

本次报告对开源情报中高级威胁活动涉及目标的国家和地域分布情况进行了分析和整理，监测显示高级威胁攻击活动几乎覆盖了全球绝大部分国家和地区。其中，开源情报中提及率最高的五个受害国家分别为：中国占比 7.4%，韩国：6.6%，美国：4.9%，巴基斯坦：3.2%，印度：3.2%。中国首次超过美国、韩国、中东等国家和地区，成为全球 APT 攻击的首要地区性目标。



▲ 图 1.3 2020 年公开高级威胁针对国家 / 地区分布情况

三、活跃高级威胁组织情况

本次报告对开源情报中所提及的所有 APT 组织及相关行动进行了分析和整理。其中，提及率最高的五个 APT 组织分别是：Lazarus：10.3%，Kimsuky：7.8%，海莲花：5.4%，Darkhotel：4.8%，蔓灵花：3.2%。下图给出了 2020 年开源情报披露的活跃 APT 组织，字体越大，被披露次数越多。

▲ 图 1.4 2020 年主要 APT 组织相关报告情况统计

四、高级威胁年度活动特点

（一）疫情热点信息成 APT 活动常用诱饵

2020 年，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。

根据奇安信威胁情报中心的监测，2020 年上半年，在针对我国的高级威胁活动中，就已经出现了大量以各类疫情热点信息为关键词的诱饵文件（诱骗吸引受害者打开的，含有恶意程序的各类文档）。2020 年 3 月下旬，奇安信曾发布《COVID-19 | 新冠病毒笼罩下的全球疫情相关网络攻击分析报告》一文，披露了 2020 年第一季度疫情相关攻击活动。

而到了 2020 年下半年以后，结合疫情热点发送鱼叉邮件或制作诱饵文件，逐步成为了全球高级持续性威胁的攻击的普遍趋势，针对我国的相关 APT 活动也进一步加剧。2020 年年中，“COVID-19 treatment methods（新冠病毒治疗方法）”等内容在 APT 活动中最为常见；而到了 2020 年末含有“covid vaccine（新冠病毒疫苗）”等内容 APT 组织诱饵文件在国外越来越多。

下图为红雨滴团队根据 APT 攻击活动相关的诱饵文件热词制作的词云图：

▲ 图 1.5 相关的诱饵热词

需要说明的是，尽管医疗卫生行业是 2020 年最受 APT 组织关注的行业，但结合疫情热点信息发起的 APT 攻击，并非只是针对医疗卫生机构，在针对政府机构和国有单位进行的攻击中，攻击诱饵也会经常会使用“疫情警告通知”“返乡疫情填报”“疫苗注射通知”等内容。

（二）供应链和远程办公成为攻击切入点

从某种程度上说，通过供应链发起的攻击，属于攻击者发动的“降维打击”，往往使防守方束手无策。2020 年，供应链攻击已经成为全球 APT 活动的流行新趋势。

常见的供应链攻击有三种方式：第一种是攻击软件供应链的各个环节，包括第三方库的引用、开发人员、产品构建阶段等；第二种是攻击和目标相关的机构，包括 IT 供应商、软件供应商、硬件供应商、合作伙伴等；第三种是针对带有签名的合法应用、预装程序植入后门，这种方法能够实现更加隐蔽的攻击立足效果。

对于软件产品来说，如果攻击者在源代码级别植入恶意代码，这些恶意代码将非常难以被发现。并且这些恶意代码在披上正规软件厂商的合法外衣后，将能更加轻易地躲过安全软件产品的检测，往往会长时间潜伏于用户机器中不被察觉。2020 年末曝光的流行网管软件厂商 SolarWinds 被植入后门代码就属于这类攻击中的经典案例。

奇安信威胁情报中心在 2020 年末还发布了软件供应链来源攻击分析报告，总结了记载详细且影响面较大的供应链攻击事件。例如，利用华硕升级程序的供应链攻击事件 ShadowHammer 行动，远程终端管理工具 Xshell 被植入后门代码事件等，均是针对生产公司内部进行入侵并篡改代码，可见一流 APT 组织的攻击活动趋势。

对远程办公相关的软件或系统发起攻击，是 2020 年全球 APT 活动的又一大特点。

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。很多远程办公系统需要通过 VPN 接入企业内部网络，一旦 VPN 的软硬件系统出现安全漏洞，就有可能为攻击者提供重要的入口。只不过从历史披露的 APT 活动来看，利用 VPN 或远程访问的脆弱性作为入口的攻击活动一直比较少见。

但是，2020 年，利用 VPN 漏洞发起的 APT 攻击非常活跃。根据国外安全机构披露，APT 组织 Fox Kitten 利用多个 VPN 漏洞向多个目标机构发起攻击，其中包括针对 Pulse Secure（CVE-2019-11510）、Fortinet FortiOS（CVE-2018-13379）和 Palo Alto Networks VPN（CVE-2018-1579）等 VPN 系统的安全漏洞。相关活动持续了整个 2020 年。

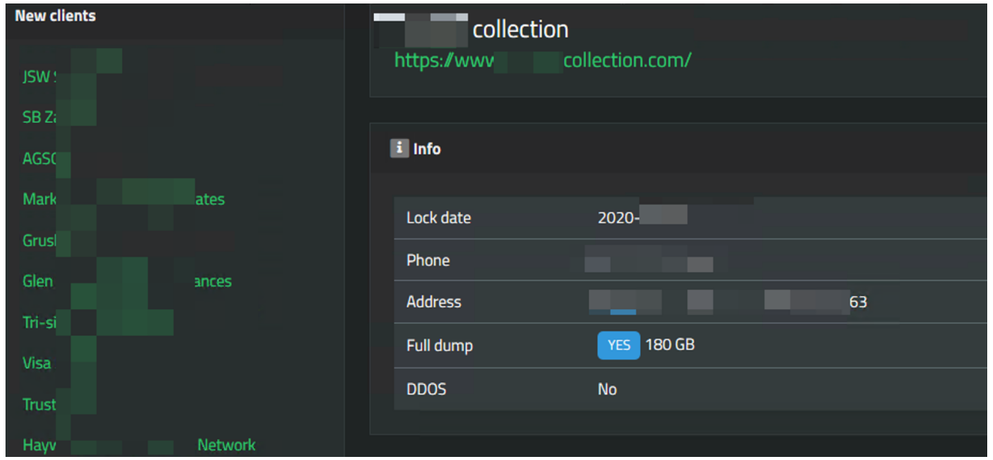
此外，2020 年 2—4 月，Darkhotel 和 Wellmess 组织也分别利用我国某著名 VPN 系统的安全漏洞进行攻击。前者的行动主要针对基层单位，后者则主要针对中国航天、研等重要机构。

除了 VPN 之外，2020 年，某全球知名视频会议软件也被 APT 组织重打包，在国内外多个下载站进行投放。

（三）定向勒索威胁成为 APT 活动新趋势

定向勒索威胁是指某些网络犯罪组织通过对特定机构的长期定向渗透，窃取机密数据，随后使用勒索软件加密相关数据，再以向公众披露相关数据相威胁，向特定机构勒索赎金的一种特殊的勒索软件攻击活动。

网络犯罪组织在瞄准一个目标后，会进行为期数月的网络渗透活动。常见攻击手法包括社会工程学、网络漏洞入侵、内鬼入侵等。在成功入侵后，攻击者会先将该目标的数据全部盗走。在完成备份后，再释放勒索软件，将目标的数据全部加密。此后，勒索软件“运营商”会将被入侵目标的部分信息公示于众，并威胁目标必须缴纳赎金，否则将曝光目标的所有数据。图 1.6 所示为某勒索软件组织公开受害者部分数据的网站示例。



▲ 图 1.6 勒索软件组织公开受害者部分数据的网站示例

由于这些针对性勒索攻击的攻击过程符合高级、持续性等威胁特征，因此我们目前认为：由某些犯罪组织发动的定向性勒索软件威胁活动，已经成为一种全球 APT 活动新形式和新趋势。

事实上，早在一两年前，定向勒索威胁的事件就已经偶有发生。但是，一方面，当时这种勒索方式与传统勒索软件攻击（只勒索，不窃密，也不泄密）相比，发生几率较低；另一方面，人们对这种攻击的整个过程也缺乏深入的研究；所以，人们并没有把这种攻击方式列入高级威胁活动分析的对象。

但是，在 2020 年，定向勒索攻击已经逐渐转变为一种新的流行趋势。尤其是自从疫情爆发开始，攻击频率就一直处于持续平稳增长态势。同时，安全工作者们经过深入研究，发现这种攻击具有明显的高级性和持续性。也正是基于这些变化，奇安信威胁情报中心已经将此类威胁纳入 APT 活动的监测与研究范围。目前，比较有名的定向勒索攻击组织有：DopplePaymer、Egregor、Netwalker、REvil（Sodinokibi）、Ryuk 等。

还有一点需要说明：监测显示，目前使用勒索软件进行定向攻击的，不仅仅是某些网络犯罪组织，还有某些具有国家背景的攻击组织，甚至是有网军的参与。有国外研究机构认为，某些国家的政府甚至已经将定向勒索活动作为一种增加财政收入的基本手段。

第二章 针对不同行业的高级持续性威胁

APT 威胁是定向性的，其会选择攻击的行业、地域、目标以及要达到的目的，这些是由 APT 组织在实施行动前制定的需要达到的阶段性目标和动机所决定的。从历史经验来看，APT 组织在一段时间内会保持其攻击目标行业的专注程度，这可能也与攻击组织在针对新的行业实施攻击时，需要时间收集和熟悉目标，并弥补自身能力与目标行业的缺失部分，以及构建相应的攻击武器库。

2019 年，金融、能源和电信这三个行业是 APT 威胁的主要行业目标。但在 2020 年，受疫情影响，APT 组织的关注度发生了转变，医疗卫生行业成为 APT 组织关注的首要目标，与疫苗研制、抗疫措施等相关的活动非常活跃。此外，网络安全、互联网、芯片与半导体等行业也成为 2020 年 APT 活动关注的新兴热点，出现了很多新的攻击特点，发生了多起影响深远的 APT 攻击事件。

一、医疗卫生行业

在新冠疫情出现之前，针对医疗卫生行业的网络攻击，主要来自网络黑产，主要目的是窃取信息、黄牛倒号和欺诈勒索（勒索软件）等。

但自 2020 年年初开始，随着新冠疫情的全球泛滥，针对疾控与防疫机构、病毒研究机构、疫苗研发机构和其他相关的医学研究机构的高级威胁活动持续不断，并使整个医疗卫生行业成为 2020 年 APT 活动关注的焦点。

2020 年 1 月末开始，来自南亚、东南亚方向的多个 APT 组织，率先针对我国医学类高校和医学科研机构展开攻击。2020 年 7 月，美国 CISA（网络安全和基础设施安全局）发布报告称：来自东欧的 APT 组织正在大规模窃取疫苗数据；其中，著名的 APT29 组织进行了针对美国、英国和加拿大的新冠研究和疫苗相关的恶意网络活动。

此外，EMA（欧洲药品管理局）于 12 月 9 日在其网站上发布了一条简讯，透露 EMA（欧洲药品管理局）遭到网络攻击；德国疫苗开发商 BioNTech 也发表声明，由该机构向监管机构提交的，其与辉瑞公司合作开发的新冠疫苗 BNT162b2 的相关资料，被存储在 EMA 服务器上，其中部分资料已被黑客入侵非法获取。

事实上，与疫苗相关的 APT 活动，不仅仅局限在疫苗研发机构。与疫苗相关的其他行业也正遭受网络攻击。2020 年 10 月，有 APT 组织假冒生物医学公司 Haier Biomedical，向与新冠疫苗冷链相关的组织

机构发起了攻击。

奇安信威胁情报中心发现，在 2020 年末曝出的 SolarWinds 供应链事件中，我国部分与疫苗相关行业机构也受到了波及。

二、网络安全行业

网络安全公司会给各类大型机构进行安全服务，如果能够掌握安全公司的安全设备 0day 漏洞，或者是获取到安全公司的权限，即可入侵客户或者是查看其客户的机密资料。只不过，由于网络安全公司的自我防御能力往往相对较强，攻击网络安全公司对于 APT 组织来说也有较大的风险，所以以往针对安全公司的 APT 活动相对较少。

但是，在 2020 年，受全球政治、经济、军事等大环境剧烈变化的影响，针对网络安全公司的定向攻击活动显著增多，这也引起了网络安全界的普遍关注。特别是由 2020 年末火眼武器库失窃事件引发的一系列相关事件，最为引人关注。此外，国内某安全公司的 VPN 软件，在 2020 年也遭受了攻击并被 APT 组织利用。相关情况已在上一章中有所论述。

（一）火眼公司网络武器库失窃事件

2020 年 12 月 8 日，美国著名网络安全公司 FireEye（火眼）发布通告称，其遭到某国家级 APT 组织入侵，并窃取了其红队渗透测试工具集。通告提到，该国家级 APT 组织的主要目的是查看火眼的客户资料。

被窃取的工具中含有火眼自己编写的黑客工具以及漏洞利用代码。此外，奇安信威胁情报中心分析火眼公布的检测规则发现，公网还存在火眼仿冒其他 APT 组织编写的木马。可想而知，这些工具落入 APT 组织手中无疑将成为另一个大杀器。

在后续调查中，火眼为了查明攻击者是如何攻入其防御系统过程中，发现了其公司购置的 SolarWinds 相关软件中存在后门，并通报了此事。

（二）SolarWinds 供应链事件

SolarWinds 是一家全球知名的网管软件服务商。2020 年 12 月 13 日被通报存在后门代码后，SolarWinds 对全球客户展开排查，经排查发现，微软、火眼、思科、VMware 等大公司均被攻击者通过该软件作为入口而成功渗透。此外，美国财政部、商务部等多个政府机构也可能已经沦陷；世界 500 强企业中，也有超过 9 成受到影响；全球至少 30 万家大型政企机构受到影响。

SolarWinds 被篡改后的后门代码被命名为 SUNBURST（Solorigate）。该后门代码会经过层层检测环境是否安全后，再采用自定义 DGA 算法进行域名生成，并通过 DNS 协议进行网络请求。在获取到 CNAME 返回的 IP 后，SUNBURST 会对攻击目标进行判断，主要通过内嵌的 IP 段进行黑白名单过滤。若目标符合则会下发第二阶段的木马，该木马被命名为 Teardrop。

奇安信威胁情报中心通过对 SUNBURST 后门代码进行分析，解码了大量 DGA 域名数据，发现许多著名的大型企业都存在受影响的 SolarWinds 相关版本软件。奇安信威胁情报中心将相关研究成果发布到推特平台，被多家国外著名安全机构在文章中引用。相关推特文章及被引用情况如图 2.1 所示。

▲ 奇安信威胁情报中心推特账号发布的 DGA 域名解码推文被多个国外安全厂商在文章中引用

西方安全界普遍认为，本次事件的幕后攻击者是著名的 APT29。著名俄罗斯安全厂商卡巴斯基也发布报告称，SolarWinds 事件中的 SUNBURST 恶意软件代码与 Turla 组织使用的 Kazuar 木马存在代码相关性。

除了核心后门代码外，SolarWinds 供应链攻击事件中实际上还涉及另一个后门代码，该后门是一个 .NET Webshell，被命名为 SUPERNOVA。该攻击的幕后攻击者目前被认为与 SUNBURST 的幕后攻击者来源不同。

三、互联网行业

2020 年，某些互联网行业企业也被 APT 组织盯上，成为了被攻击的目标。

（一）网络社区

2020 年，多个推特名人大 V 账户遭黑客攻击，发送比特币诈骗信息，事后复盘发现黑客通过客服渠道作为入口进行社会工程学攻击。相关活动虽然不是知名 APT 组织所为，但其攻击过程也具有明显的高级性和持续性。

除了网络社区本身存在漏洞问题而被入侵外，有多个 APT 组织在 2020 年频繁使用某知名招聘社区平台进行钓鱼攻击。例如，Lazarus 组织通过在某全球知名招聘社区注册账号，伪造成攻击目标希望应聘公司的员工，再通过平台渠道发送带有恶意代码的表格让目标点击填写。

（二）即时通信

WhatsApp、iMessage 的 0day 漏洞被网络军火商 NSO Group 进行售卖，中东地区国家情报机构使用这些漏洞进行攻击和监控。

以 Lazarus 组织为例，由于 WhatsApp 仅需手机号码即可添加好友，当该组织黑客在招聘社区平台上获取到其计划诱骗目标的手机号后，会通过该 App 作为通信入口进行交谈，并在交谈过程中发送恶意软件。

四、半导体行业

半导体行业由于其技术高新性，并且产业极具供应链属性（上游制造半导体设备与材料，中游进行芯片设计，下游进行晶圆代工和封装测试），若其中运作的一环受到网络攻击，那么全球的半导体供应链将受到影响。2020 年，全球多家芯片公司和晶圆代工厂遭受高级威胁攻击导致停产，数据泄露严重。

晶圆代工类：晶圆代工厂龙头 X-FAB 被定向性勒索攻击，系统加密导致停产。以色列晶圆代工商高塔（TowerJazz）半导体遭受 APT 攻击，服务器和制造部门停止运转。

芯片行业：英特尔公司 20GB 芯片数据泄露，内含机密文件以及设计图。

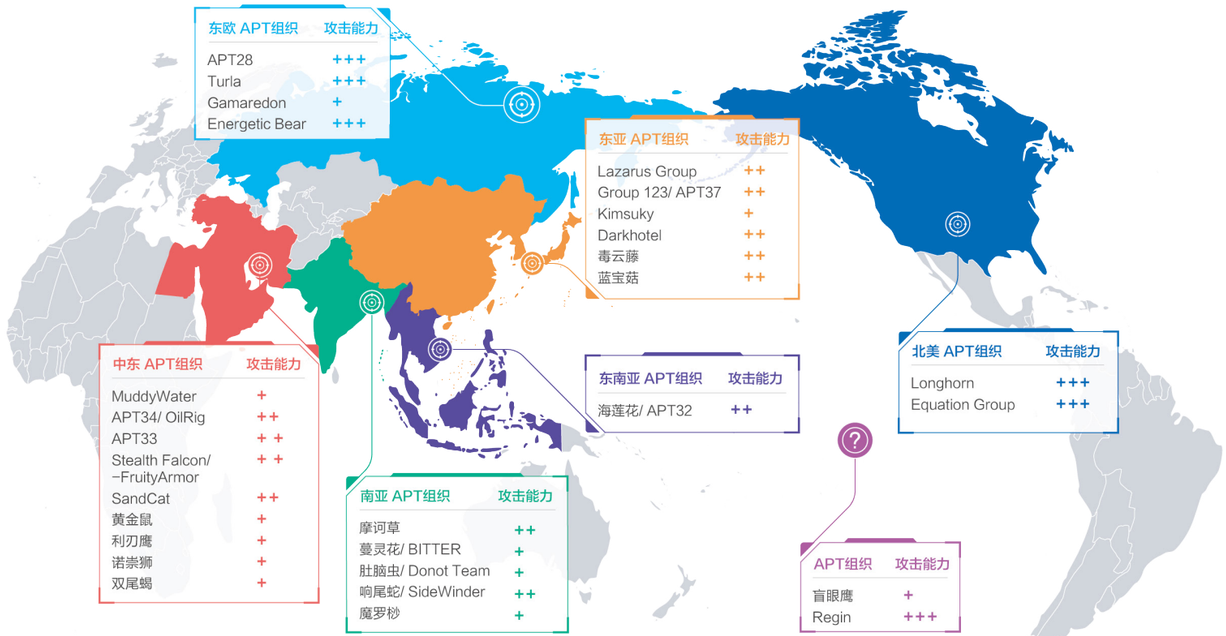
半导体厂商：台湾多家半导体厂商被 APT 组织攻击，这些组织的目的是窃取有关集成电路芯片、软件开发工具包、集成电路设计、源代码等。韩国半导体知名企业 SK 海力士遭受定向性勒索软件攻击，数据遭泄露。

从这几起事件可以看出，2020 年针对半导体行业的 APT 攻击，不仅仅局限于窃取技术资产，敛财也是其重要目的。

第三章 不同地区活跃的高级攻击组织

地域分析是 APT 研究的重要方面。一方面，同一地域范围的 APT 组织和 APT 活动常常出现一些重叠，其可能针对相似的攻击目标或者使用类似的 TTP；另一方面，同一地区发生的很多 APT 活动，都与地缘政治因素密切相关，这对于分析 APT 活动的意图和动机很有帮助。

图 3.1 列举了 2020 年全球各地区主要活跃的 APT 组织，全球主要 APT 组织列表也可以参见附录 1。



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

▲ 图 3.1 全球 APT 组织分布情况

东亚地区的组织与行动

East Asia

2020 年被公开披露最多的三个东亚地区活跃的 APT 组织为 Lazarus、Kimsuky 和 Darkhotel。其中，azarus 一直作为东亚地区最为活跃的 APT 组织，其目标是全球性的，攻击行业也涉及极广。Kimsuky 组织则更专注于政府相关部门，多次以美国大选为诱饵开展攻击。表 3.1 所示为东亚地区主要活跃 APT 组织简介。

2013

Kimsuky

最早活动时间：2013
公开披露时间：2013

该组织致力于以韩国智库、工业、核电运营商和统一部为间谍活动目标，并且与 Group 123 组织存在一定关联。

2014

Darkhotel

最早活动时间：2004
公开披露时间：2014

2014 年披露的攻击组织，擅长利用浏览器的 0day 和 Nday 漏洞开展攻击活动。最早活跃于 2004 年。

2016

Lazarus

最早活动时间：2009
公开披露时间：2016

该组织最早的攻击活动可以追溯到 2009 年，包括针对韩国的 DarkSeoul,2014 年针对 SONY 事件。近几年来，该组织主要针对全球银行、加密货币等目标开展攻击活动。

2016

Group123

最早活动时间：2012
公开披露时间：2016

Group 123 主要针对韩国的公共和私营部门。2017 年，其目标范围扩展到了朝鲜半岛以外的地区，包括日本、越南和中东，并扩展到了更广泛的行业垂直领域，包括化工、电子、航空航天、汽车和医疗保健实体。

2018

毒云藤

最早活动时间：2007
公开披露时间：2018

毒云藤是在 2018 年被奇安信公开披露的 APT 组织，该组织长期针对国内国防、政府、科技和教育领域的重要机构实施网络间谍攻击活动，最早的活动可以追溯到 2007 年。

▲ 东亚活跃 APT 组织简介

▪ APT 组织：Lazarus

Lazarus 一直被认为是一个来自东亚地区的具有东亚某国政府背景的 APT 组织，同时也一直被安全厂商作为疑似该国 APT 活动归属总称。某些国外安全厂商也将其该组织针对金融、银行行业的攻击归属作为一个子组织来跟踪。2020 年，该组织仍旧针对全球性的金融、银行、数字货币、政府等行业开展攻击活动。针对数字货币的攻击尤为明显，其多次通过制造虚假的交易场所网站分发恶意代码。同时，据公开情报透露，长年针对数字货币的“危险密码”组织也与 Lazarus 存在关联。

2020 年，Lazarus 组织被披露通过多个知名社交媒体，创建多个虚假账号组成社交圈，以此伪装为波音等著名航空航天等军工单位人员，对相关领域专业人士发送附有恶意代码的招聘信息。奇安信威胁情报中心整理了部分 Lazarus 组织利用招聘信息的诱饵文档如图 3.2 所示。

▲ 图 3.2 Lazarus 组织发布的招聘诱饵文档

Lazarus 组织在 2020 年被发现开始采用信用卡钓鱼、勒索软件、供应链攻击等新型攻击方式。作为最老牌且活跃的 APT 组织之一，除了更新其攻击手法以外，该组织攻击工具集也保持了频繁开发与更新。表 3.2 列举了 2020 年度 Lazarus 被披露的新增网络武器库。

攻击工具名称	功能说明
MATA	针对 Windows、macOS、Liunx 三个平台的攻击框架
BISTROMATH	一款全功能 RAT
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

▲ 表 3.2 2020 年度 Lazarus 新增网络武器库

▪ APT 组织：Group123

Group123 作为另一个东亚老牌 APT 组织，2020 年度被披露活动较少。而与 Group123 具有相同背景归属的 Kimsuky、Konni 开始活动频繁。Kimsuky 组织擅长利用政治热点新闻作为诱饵开展攻击活动。

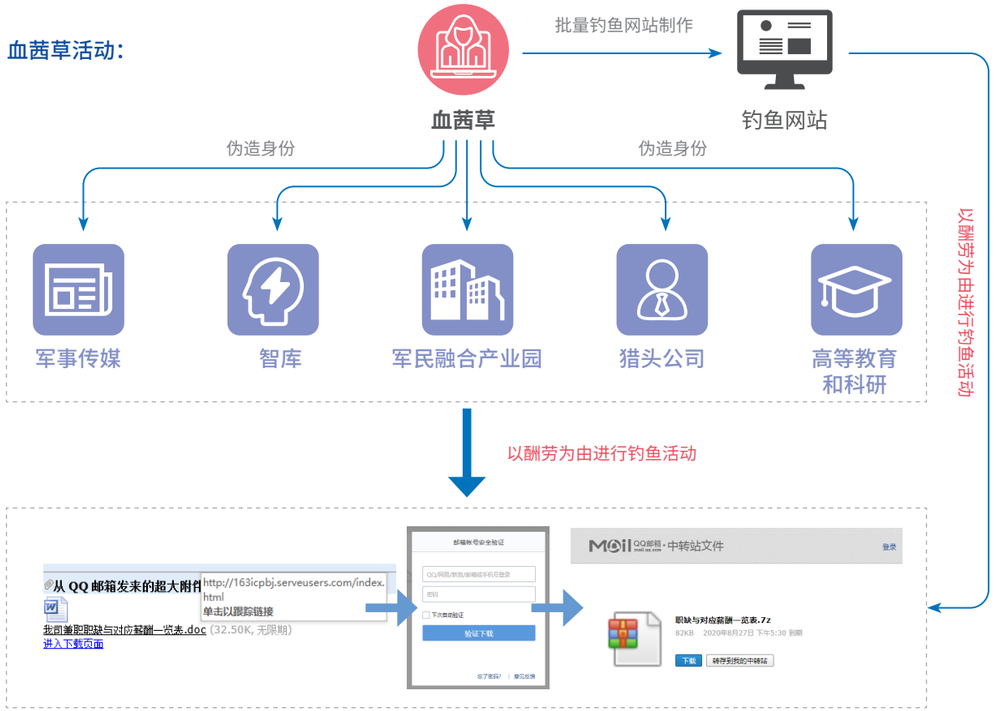
例如，在美国大选期间，多次以投票预测、拜登政策相关大选信息为诱饵开展攻击。同时，据韩国安全公司发现，Konni 组织与 Kimsuky 存在基础设施重叠。

▪ APT 组织：Darkhotel

Darkhotel 是东亚地区另一个活跃的 APT 组织，其长期针对包括中国在内的多个东亚国家实施攻击行动，擅长利用 0day 和 1day 漏洞实施攻击。该组织 2020 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。奇安信威胁情报中心列举了东亚地区 2020 年热点攻击活动，如表 3.3 所示。

▲ 表 3.3 2020 年东亚地区热点攻击活动

2020 年，奇安信威胁情报中心命名了一个新的华语 APT 组织活动：血茜草活动，该活动由毒云藤发起，此次攻击活动趋向渔网化，通过批量与定向投方相结合，采取信息探测的方式辅助下一步的定点攻击。主要分为三种攻击类型：钓鱼网站钓鱼、诱饵引诱钓鱼和恶意附件式钓鱼攻击，根据我们观察，血茜草活动中伪装了多个具备鲜明特色的角色，如智库类目标、军民融合产业园、军事杂志、公务员类猎头公司等等。下图展示了血茜草活动中常用的攻击手法。



▲ 血茜草活动常用攻击手法

东南亚地区的组织与行动
Southeast Asia

海莲花组织依然是在东南亚地区最为活跃的 APT 组织，其在 2020 年依然保持较高的活动频率。该组织已经由过去的网络间谍活动延伸至商业情报窃取领域，如互联网行业。并首次发现了该组织开始在受害者计算机中部署挖矿程序。

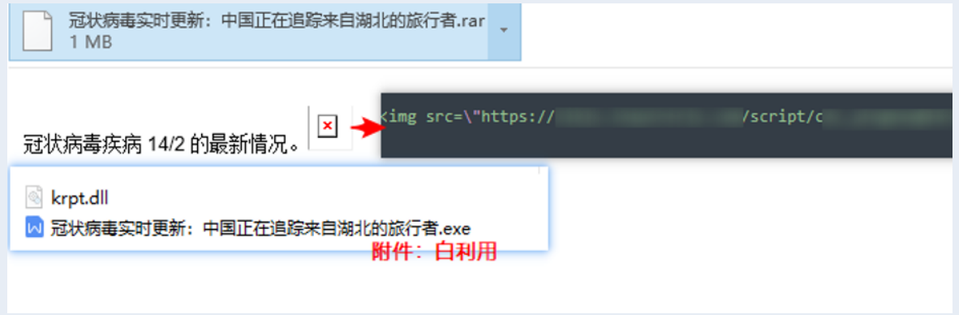
▪ APT 组织：海莲花

组织名	海莲花
公开披露时间	2015 年
最早活动时间	2012 年
组织简介	海莲花组织是由奇安信威胁情报中心最早披露并命名的一个 APT 组织，其自 2012 年 4 月起，该组织针对中国政府、科研院所、海事机构、海域建设、航运企业等相关重要领域展开了有组织、有计划、有针对性的长时间不间断攻击。

▲ 表 3.4 东南亚主要 APT 组织简介

海莲花组织在 2020 年全年持续不断地针对我国各行各业重点单位进行攻击，攻击单位不局限于政府部委、国防、海事等单位，还有一些大型互联网公司也惨遭毒手。

从 2020 年年初疫情爆发开始，海莲花就开始针对我国医疗行业单位进行邮件投递攻击，制造带有探针追踪的邮件，如图 3.4 所示。



▲ 图 3.4 海莲花组织利用疫情信息投递的邮件

2020 年下半年海莲花组织继续针对我国单位继续发起攻击，且其攻击木马开始定制化，如采用受害者计算机用户名等信息加密恶意载荷，采用“白利用”的方式加载执行恶意载荷等。表 3.5 列举了部分奇安信发现的海莲花组织针对国内的白利用。

白程序	恶意 DLL
KVHistory.exe(江民)	KVInstall.dll
AlibabaProtect.exe(阿里)	Report.dll
AliIM.exe(淘宝旺旺)	UClientStartup.dll
SogouIMEBroker.exe（搜狗输入法）	UClientStartup.dll
LBTWizGi.exe（罗技组件）	LBTServ.dll
SearchProtocolHost.exe	TmDbgLog.dll
SogouCloud.exe（搜狗输入法）	LBTServ.dll

▲ 表 3.5 海莲花组织常用白利用

2020 年，海莲花组织除针对中国境内开展攻击活动以外，也被公开披露了多起针对柬埔寨、孟加拉国等国家地区的攻击活动。奇安信威胁情报中心整理了 2020 年度海莲花组织部分热点攻击活动如表 3.6 所示。

2020/03/16

披露来源：微步在线
APT 组织：海莲花

海莲花组织利用新冠肺炎疫情，禽流感的攻击活动

2020/04/29

披露来源：卡巴斯基
APT 组织：海莲花

PhantomLance 行动，与海莲花组织存在基础设施重叠的 Android 端攻击活动

2020/08/20

披露来源：微步在线
APT 组织：海莲花

该组织利用白利用，（SFX）RAR 自解压文件和携带宏代码的 MIME 格式文档方式的攻击活动

2020/11/06

披露来源：Volexity
APT 组织：海莲花

利用社交媒体分发钓鱼网站的攻击行动

2020/11/27

披露来源：趋势科技
APT 组织：海莲花

海莲花新型 Macos 后门分析

2020/12/10

披露来源：Facebook
APT 组织：海莲花

facebook 删除海莲花组织相关账户，并将其与越南 IT 公司关联起来

▲ 表 3.6 2020 年东南亚地区热点攻击活动

南亚地区的组织与行动
South Asia

奇安信威胁情报中心

2013

摩诃草

最早活动时间：2009
公开披露时间：2013

最早由 Norman 曝光，具备 Windows、Android、macOS 三平台攻击能力，主要针对中国、巴基斯坦等亚洲地区国家进行网络间谍活动，以窃取敏感信息为主。

2016

蔓灵花

最早活动时间：2013
公开披露时间：2016

曾对中国、巴基斯坦等相关目标实施 APT 攻击。奇安信在跟踪该组织后续过程种发现其使用 InPage 漏洞，并与摩诃草、魔罗桫存在关联。

2016

魔罗桫

最早活动时间：2013
公开披露时间：2016

主要针对南亚各国的政府、军事等行业目标进行攻击。其攻击会部署定制后门及定制文件窃取器从受害者的系统中窃取文件。

2016

Transparent Tribe

最早活动时间：2012
公开披露时间：2016

主要瞄准印度的军队或者相关组织开展攻击活动。

2017

肚脑虫

最早活动时间：2016
公开披露时间：2017

以巴基斯坦等南亚地区国家政府作为其攻击目标，攻击工具主要使用 yty 和 EHDevel 两套恶意框架。

2018

Sidewinder

最早活动时间：2012
公开披露时间：2018

主要针对包括巴基斯坦和中国在内的东南亚国家，常使用已知漏洞 (CVE-2017-11882) 开展攻击活动。

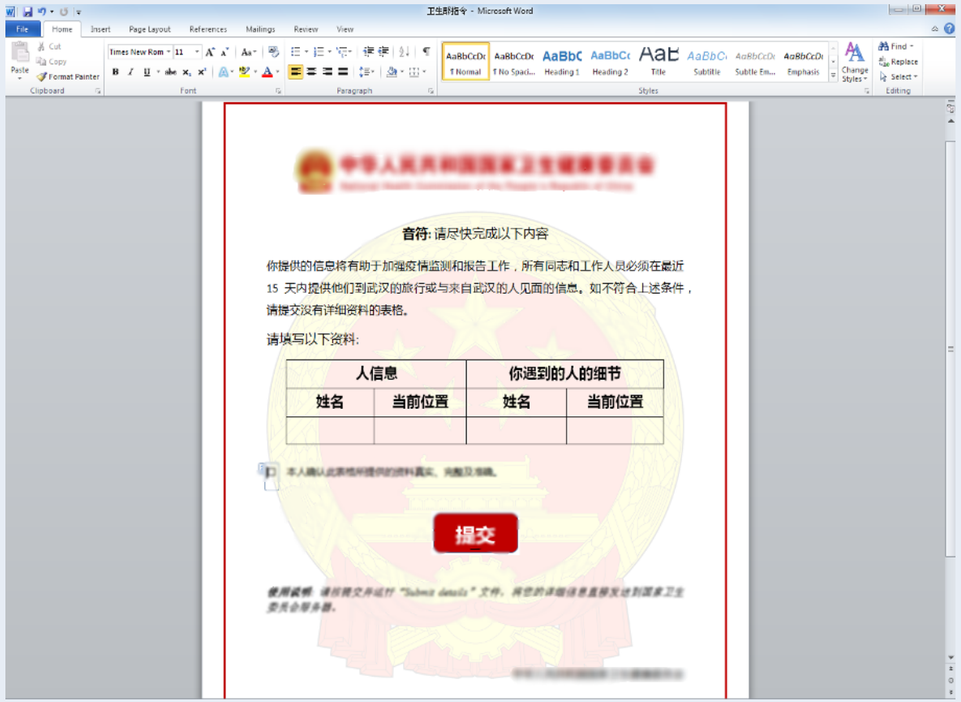
▲ 表 3.7 南亚地区主要 APT 组织简介

南亚 APT 组织大多利用携带公式编辑器漏洞的诱饵文档为攻击入口，同时都基本具备针对 Windows 和 Android 平台的攻击工具。其中摩诃草、蔓灵花、响尾蛇、魔罗桫等组织，长期针对中国境内开展攻击活动。肚脑虫组织则更多专注于巴基斯坦等周边国家。

▪ APT 组织：摩诃草

摩诃草组织擅长利用时事热点为诱饵开展攻击活动，2020 年疫情初期，摩诃草组织是被公开披露的第一个利用疫情诱饵针对我国重点医疗政府单位的 APT 组织。

图 3.5 所示为摩诃草组织利用疫情信息针对国内的部分样本诱饵信息。



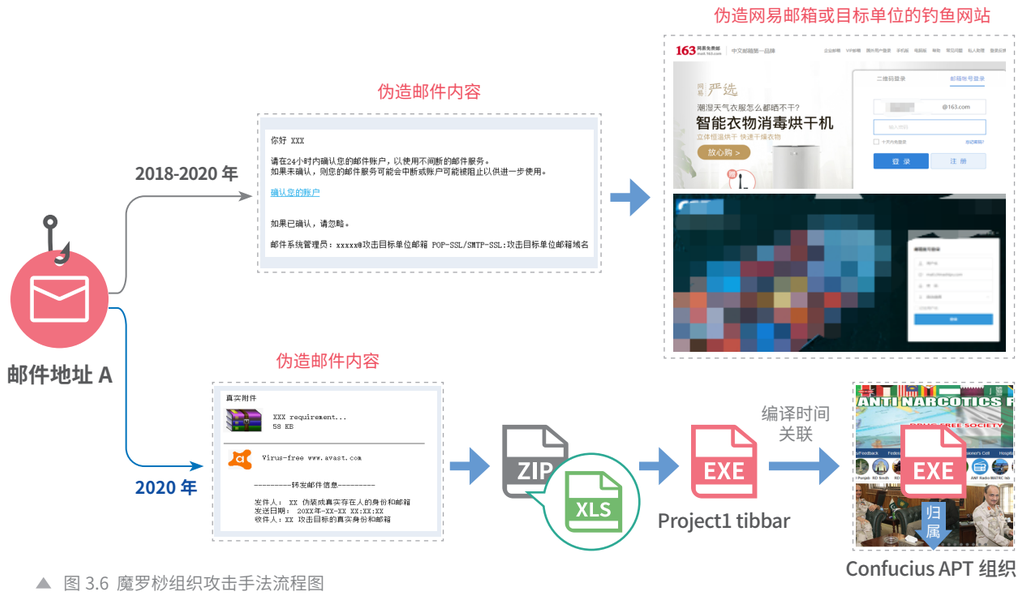
▲ 图 3.5 摩诃草组织疫情样本诱饵信息

▪ APT 组织：蔓灵花 & 响尾蛇

在 2020 年，整体而言，蔓灵花组织与响尾蛇组织攻击手法未发生较大改变。值得注意的是，响尾蛇组织在利用疫情诱饵针对我国顶尖高校的攻击活动中，首次使用了 IE 浏览器漏洞 CVE-2020-0674。

▪ APT 组织：魔罗桫

2020 年，奇安信威胁情报中心曝光了一个新命名的该地区 APT 组织——魔罗桫。该组织活跃在南亚地区，一直持续针对中国、巴基斯坦等国的国防、军工、外交等单位进行攻击，擅长制造钓鱼网站并配合鱼叉邮件进行攻击，恶意软件主要针对 Windows 和 Android 双平台。图 3.6 所示为魔罗桫组织攻击手法流程图。



▲ 图 3.6 魔罗杪组织攻击手法流程图

表 3.8 总结了上述南亚 APT 组织在 2020 年度的主要攻击活动：

2020/02/04
披露来源：360
APT 组织：摩诃草
借新冠疫情对我国医疗机构发起定向攻击

2020/02/24
披露来源：微步在线
APT 组织：摩诃草
利用升级的武器库针对我国境内的攻击

2020/02/27
披露来源：腾讯
APT 组织：蔓灵花
蔓灵花 (BITTER)APT 组织 2020 年初针对中国境内最新攻击活动

2020/04/28
披露来源：奇安信
APT 组织：肚脑虫
针对南亚周边国家地区的攻击活动分析

2020/05/20
披露来源：奇安信
APT 组织：响尾蛇
制作新冠疫情相关诱饵针对周边国家的攻击

2020/06/18
披露来源：Bitdefender
APT 组织：蔓灵花
移动武器库更新

2020/06/30
披露来源：奇安信
APT 组织：肚脑虫
数字武器库升级，增加 Loader 以绕过杀软检测

2020/08/31
披露来源：安恒
APT 组织：摩诃草
武器库新增 CVE-2019-0808 提权模块

2020/09/01
披露来源：奇安信
APT 组织：摩诃草
利用边境争端问题的攻击活动

2020/09/14
披露来源：奇安信
APT 组织：蔓灵花
疑似 BITTER 组织利用 LNK 文件的攻击活动

2020/10/19
披露来源：360
APT 组织：响尾蛇
利用 WebSocket 隧道的新型攻击样本分析

2020/10/22
披露来源：奇安信
APT 组织：蔓灵花
利用 CHM 文件针对境内的攻击活动

2020/10/27
披露来源：奇安信
APT 组织：响尾蛇
利用巴菲双边协议为诱饵的攻击

2020/10/29
披露来源：思科
APT 组织：肚脑虫
利用 Google Firebase Cloud Messaging 进行传播

2020/10/30
披露来源：360
APT 组织：肚脑虫
针对巴基斯坦军事人员的最新攻击活动

2020/11/19
披露来源：安恒
APT 组织：响尾蛇
以一带一路为诱饵针对我国的攻击

2020/12/04
披露来源：深信服
APT 组织：响尾蛇
伪装成 NDC 印度国防学院的攻击

2020/12/09
披露来源：趋势科技
APT 组织：响尾蛇
针对阿富汗，巴基斯坦攻击活动综述

▲ 表 3.8 南亚地区热点攻击活动

▪ APT 组织：透明部落（Transparent Tribe）

2020 年，南亚另一 APT 组织透明部落（Transparent Tribe）也活动频繁，年初多利用新冠肺炎相关信息为诱饵针对印度实施攻击。奇安信威胁情报中心移动安全团队在 2020 年 8 月首发披露了该组织在移动端的攻击活动。另有分析显示，伪装成响尾蛇组织针对印度的 Sidecopy 行动疑似也与透明部落存在联系。

东欧地区的组织与行动
Eastern Europe

东欧地区老牌 APT 组织 APT28、APT29、Turla 依旧保持着其高超的技术性与隐匿性，鲜有公开报告对其进行披露。同时，诸如针对东欧机构攻击长达九年的 XDSPY 组织，针对工业的恶意软件集 MontysThree 开始进入视野。表 3.9 所示为东欧地区活跃的组织简介。

2013

APT29

最早活动时间：2008
公开披露时间：2013

该组织的主要目标为西亚、中亚、东非和中东的政府部门和机构。其被认为在 2015 年夏季攻击了美国 DNC。

2014

APT28

最早活动时间：2004
公开披露时间：2014

该组织历史活动非常频繁，主要针对政府，军事和安全组织，特别是与高加索和北约结盟的国家开展网络间谍活动。

2014

Turla

最早活动时间：2007
公开披露时间：2014

该组织拥有非常复杂的 TTP，其受害者覆盖超过 45 个国家，常针对政府、大使馆、军事、教育、研究和制药公司实施鱼叉和水坑攻击。

2015

Gamaredon

最早活动时间：2013
公开披露时间：2015

主要针对乌克兰执法部门、政府机构和军事力量进行间谍活动和情报收集等攻击。Operation Armageddon 行动与该组织有关。

2020

XDSpy

最早活动时间：2011
公开披露时间：2020

其针对东欧和巴尔干地区，主要目标为政府、军队、外交部以及私营公司。

▲ 表 3.9 东欧地区主要 APT 组织简介

▪ APT 组织：WELLMESS

2020 年，美国、加拿大等国家五部门联合发布 WELLMESS 针对新冠肺炎疫苗相关机构的攻击，并称其与 APT29 存在关联。

奇安信威胁情报中心整理了 2020 年度东欧 APT 组织热点攻击活动，如表 3.10 所示。

2020/01/04

披露来源：Area 1 Security
APT 组织：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

2020/02/05

披露来源：SentinelOne
APT 组织：Gamaredon

长期针对乌克兰安全机构的攻击

2020/02/15

披露来源：奥地利外交部
APT 组织：Turla

奥地利成功防御 Turla 攻击，并破解了 Turla 投递载荷的加密通信方式

2020/03/12

披露来源：ESET
APT 组织：Turla

亚美尼亚几个网站被披露被 Turla 实施水坑攻击，植入 js 并分发恶意 Flash 更新

2020/03/19
披露来源：趋势科技
APT 组织：APT28
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

2020/04/09
披露来源：安恒
APT 组织：WELLMESS
利用某 VPN 漏洞针对国内的攻击活动

2020/04/15
披露来源：ESET
APT 组织：Energetic Bear
针对旧金山两个机场实施了 APT 攻击活动。

2020/04/16
披露来源：思科
APT 组织：PoetRAT
利用俄语打包软件制作的 PoetRAT 针对阿塞拜疆的攻击活动

2020/05/14
披露来源：Leonardocompany
APT 组织：Turla
“Penquin_x64“ 变种分析，国外安全厂商称当今欧洲和美国仍有数十个 Internet 主机服务受到影响

2020/05/26
披露来源：ESET
APT 组织：Turla
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

2020/06/18
披露来源：ESET
APT 组织：InvisiMole
东欧地区活跃的 InvisiMole 疑似与 Gamaredon 开展活动，在某受害者机器上，研究人员发现 Gamaredon Group 的 .NET 下载器下载执行了 InvisiMole 组织的 TCP 下载器。

2020/07/01
披露来源：360
APT 组织：APT28
利针对欧洲的攻击活动

2020/07/14
披露来源：Telsy
APT 组织：Turla
TURLA 更新其武器库：“NEWPASS”恶意软件投入攻击

2020/07/16
披露来源：CISA 等
APT 组织：WELLMESS
美国，加拿大等国家五部门联合发布 APT29 针对新冠疫苗开发机构的攻击活动，并提出 WELLMESS 与 APT29 存在联系

2020/08/18
披露来源：奇安信
APT 组织：APT28
奇安信披露 APT28 针对阿塞拜疆知名人士的定向攻击活动

2020/09/10
披露来源：微软
APT 组织：APT28
安全厂商称 APT28 参与针对美国大选的攻击活动

2020/10/02
披露来源：ESET
APT 组织：XDSPY
针对东欧政府机构长达九年的攻击活动

▲ 表 3.10 2020 东欧 APT 组织热点攻击活动

其中最为典型的事件案例还是奥地利政府针对 Turla 组织在 2020 年 1 月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。

中东地区的组织与行动
Middle East

中东地区具有着极为复杂的政治外交局势和宗教文化差异。该地区充满了各种疑似政府背景的情报监控和网络间谍活动。2020 年，奇安信威胁情报中心披露了在中东地区活跃的两个新 APT 组织——诺崇师和利刃鹰。

奇安信威胁情报中心

2015

双尾蝎

最早活动时间：2011
公开披露时间：2015

该组织攻击范围主要为中东地区，其针对 Windows 和 Android 双平台采取鱼叉或水坑等攻击方式配合社会工程学手段进行渗透，向政府、金融、媒体、能源、军事等特定目标人群进行攻击。

2016

APT34

最早活动时间：2014
公开披露时间：2016

其针对中东地区实施攻击，攻击目标包括金融、政府、能源、化工和电信等行业。该组织过去以 APT34 和 OilRig 两个不同的名称分别进行追踪分析。

2017

APT33

最早活动时间：2013
公开披露时间：2017

APT33 是 FireEye 披露的 APT 组织，攻击目标包括美国、沙特阿拉伯和韩国，主要针对航空和能源领域实施攻击活动。

2017

MuddyWater

最早活动时间：2017
公开披露时间：2017

主要针对中东实施网络间谍活动，也针对欧洲和北美国家。其攻击目标包括电信、政府 (IT 服务) 和石油部门。主要使用基于 PowerShell 的初始阶段后门，也被称为 POWERSTATS。

2020

诺崇师

最早活动时间：2013
公开披露时间：2020

为奇安信披露的组织，活跃在中东地区，一直持续针对阿拉伯用户、什叶派及评论人士进行攻击，旨在让被攻击者的社交平台账号变成“沉默账号”。

2020

利刃鹰

最早活动时间：2019
公开披露时间：2020

该组织针对“伊斯兰国”、基地组织、库尔德族群和土库曼族群进行持续攻击控制活动。

▲ 表 3.11 中东地区主要 APT 组织简介

▪ APT 组织：双尾蝎

双尾蝎组织，是自 2016 年 5 月起长期针对巴勒斯坦的攻击组织。2020 年，奇安信威胁情报中心多次公开披露该组织在 Windows 和 Android 双平台上新的攻击样本。新的样本较以往的代码结构，通信方式未发生较大改变，依旧习惯采用人名等作为指令，C2 服务器路径也变化不大。同时，也有国外安全机构披露了该组织新的 Python 后门。

▪ APT 组织：Muddywater

老牌 APT 组织 Muddywater、APT33、APT34 依旧是中东地区三个比较活跃的组织，但由于其攻击武器库泄露，这些组织似乎都开始进行攻击手法、武器工具集的更新。结合公开情报，我们整理了中东地区过去一点主要攻击活动如表 3.12 所示。

2020/01/09
披露来源：ClearSky
APT 组织：APT34
APT34 使用的新的基于 PowerShell 的攻击程序 PowDesk

2020/02/12
披露来源：Telsy
APT 组织：APT33
APT33 开发的新的 .Net 载荷程序 POWERBAND

2020/02/16
披露来源：ClearSky
APT 组织：Fox Kitten
持续三年的攻击活动，疑似与 APT33,APT34 存在联系

2020/02/28
披露来源：奇安信
APT 组织：诺崇狮
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

2020/03/02
披露来源：Yoroi
APT 组织：APT34
针对黎巴嫩政府的攻击活动 , 并更新了 Karkoff 载荷

2020/04/19
披露来源：启明星辰
APT 组织：APT34
APT34 更新其后门工具 TONEDEAF

2020/05/19
披露来源：赛门铁克
APT 组织：OilRig
针对南亚电信运营商的攻击活动

2020/06/29
披露来源：思科
APT 组织：StrongPity
StrongPity 组织扩大攻击范围，开始针对哥伦比亚，印度，加拿大和越南开展攻击活动

2020/07/23
披露来源：Palo Alto
APT 组织：OilRIg
针对中东电信组织的攻击活动

2020/08/27
披露来源：ClearSky
APT 组织：APT35
攻击者伪装为德国之声和犹太日报的攻击活动

2020/09/18
披露来源：CheckPoint
APT 组织：Rampant Kitten
针对伊朗侨民和不同政见者的攻击活动

2020/10/19
披露来源：奇安信
APT 组织：双尾蝎
利用伪造社交软件等针对多平台的攻击活动

2020/10/20
披露来源：Telsy
APT 组织：Muddywater
伪装为知名公司招聘针对航空领域的攻击活动

2020/10/29
披露来源：360
APT 组织：StrongPity
针对我国境内重要机构的攻击活动

2020/11/30
披露来源：奇安信
APT 组织：利刃鹰
在移动端针对中东地区的攻击活动

2020/12/09
披露来源：360
APT 组织：Domestic Kitten
Domestic Kitten 伪装为居鲁士大帝等相关 APP 针对中东的攻击活动

▲ 表 3.12 2020 中东 APT 组织热点攻击活动

其他地区的组织与行动
Other areas in World

南美、北非等地区的 APT 活动也比较活跃，但往往容易被忽视。奇安信披露的南美地区 APT 组织“盲眼鹰”自 2018 年起，持续针对哥伦比亚地区开展攻击活动。同时，国内安全公司也披露了一个北非地区的 APT 组织——北非狐，该组织主要针对阿拉伯地区开展攻击活动。

2020 年，雇佣军性质的高级威胁组织正在成为趋势，这些组织拥有近乎 APT 组织的高级攻击技术，并会尝试制作与公开已知的 APT 组织相关联的假旗，通常侧重于企业间谍活动。2020 年，国外安全机构商披露了包括 Deathstalker、RedCurl、CostaRicto 在内的多个雇佣军团体的相关活动。奇安信威胁情报中心整理上述组织的相关简介，如表 3.14 所示。

2019

盲眼鹰

最早活动时间：2018
公开披露时间：2019

从 2018 年 4 月起至今，一个疑似来自南美洲的 APT 组织盲眼鹰（APT-C-36）针对哥伦比亚政府机构和大型公司（金融、石油、制造等行业）等重要领域展开了有组织、有计划、针对性的长期不间断攻击。

2020

北非狐

最早活动时间：2017
公开披露时间：2020

针对阿拉伯语地区的长达三年的多次网络攻击活动，攻击平台主要为 Windows 和 Android。

2020

DeathStalker

最早活动时间：2012
公开披露时间：2020

针对事务所和金融公司，提供出租服务。该组织采用基于 powershell 的 Powersing 的工具。该组织的攻击目标可能是根据目标价值或者客户要求选择目标。

2020

RedCurl

最早活动时间：2018
公开披露时间：2020

RedCurl 的主要目标是从受害者的基础设施和企业电子邮件中窃取文档。

2020

CostaRicto

最早活动时间：2020
公开披露时间：2020

雇佣组织，目标集中在东南亚地区，主要针对金融行业开展攻击活动。

▲ 表 3.14 其他地区主要 APT 组织简介

第四章 针对中国高级持续性威胁

2020 年，中国首次超过美国、韩国、中东等国家和地区，成为全球 APT 活动的首要地区性目标。本章主要就 2020 年针对中国的高级持续性威胁活动进行独立的整理和分析。

2020 年，奇安信威胁情报中心追踪了若干起针对中国的重大 APT 组织攻击活动，其中主要以东亚、南亚、东南亚三个方向的 APT 组织为主。

一、东亚地区组织对中国的攻击活动

2020 年，名为毒云藤的华语 APT 组织持续性出击，制造了大量仿冒网站进行钓鱼。奇安信威胁情报中心将此系列活动命名为血茜草行动。

在 2020 年年初，血茜草行动主要以伪造国内多款知名邮箱服务的网盘网站为主，并且结合疫情进行诱饵的构造，主要钓鱼模式为：当受害者输入邮箱账号密码，网站会自动跳转至恶意文件下载页面。

在 2020 年年中，血茜草行动开始转向更具针对性的攻击，主要分为三种攻击类型：钓鱼网站钓鱼、诱饵引诱钓鱼和恶意附件式鱼叉攻击。根据奇安信威胁情报中心监测，血茜草行动中伪装了多个具备东北亚地区特色的角色，如智库类目标、军民融合产业园、军事杂志、公务员类猎头公司，等等。

在 2020 年年末，血茜草行动开始针对我国高校和科研机构进行仿冒钓鱼攻击，并且出现批量注册批量仿冒的现象。

此外，值得注意的是，通过分析发现，血茜草行动中存在创新性的攻击方法：传统模式中，攻击者主要通过诱骗目标，使其点击恶意程序，之后自行设法获取情报信息。而新的攻击方式主要体现在，攻击者通过诱骗目标，使之通过“回复信息”的方式，主动将敏感情报发送给攻击者。

二、南亚地区组织对中国的攻击活动

南亚 APT 组织针对我国的攻击贯穿 2020 年全年，并且不同的 APT 组织存在不同的职能。

在 2020 年年初，摩诃草（PatchWork）在疫情出现开始就持续制造诱饵针对我国进行攻击，制造诱饵

包括武汉疫情、返乡登记表等。

而响尾蛇（Sidewinder）、蔓灵花（Bitter）、魔罗纱（Confucius）组织的攻击则是贯穿全年。其中，蔓灵花（Bitter）和魔罗纱（Confucius）组织既会制造钓鱼仿冒网站，又会生成 PC 和移动端的木马进行攻击，两者都主要针对政府机构、军工企业、核能行业、商贸会议、通信运营商等进行攻击。
而响尾蛇（Sidewinder）则有所不同，其沿用以前的攻击框架，并融入 IE Nday 漏洞来针对高校进行攻击，具有一定的创新性。

在 2020 年年末，蔓灵花（Bitter）组织集中发起了一次大型钓鱼活动，主要围绕我国外交单位进行“邮件 + 钓鱼仿冒网站”的攻击，同时邮件和网站主题涉及多个热门主题，如疫情、直播、服务维护和异常、外交文件等，极具诱惑性。

三、东南亚地区组织对中国的攻击活动

海莲花组织在 2020 年依旧针对我国海洋、油气类行业和政府单位进行攻击，除此之外，其还开始针对我国互联网和软件公司进行攻击。

海莲花组织在 2020 年转变了攻击思路。该组织大幅降低了使用鱼叉邮件攻击的频率，转而采取网络渗透的方式（例如 VPN）进行入侵，并在入侵到内网后进行一系列的持久化与横向移动操作。

奇安信威胁情报中心监测发现，海莲花组织挖掘了数十个国产软件的“白利用”，并将其用于内网渗透过程中。在内网渗透过程中，该组织会记录每台控制的主机信息，生成日志并进行回传，从而方便进行下一步的横向移动。

此外，与往年不同的是，2020 年海莲花组织开始积极使用 Nday 漏洞进行攻击，这些漏洞平日不会被人关注到，漏洞修复率低，因此在制造出漏洞 exp 后，其可以进行批量入侵获取权限。

除了捕获到海莲花积极利用 Nday 漏洞攻击活动外，奇安信威胁情报中心在 2020 年还捕获到该组织使用 0day 漏洞进行内网渗透攻击活动，从该活动发现，当海莲花遇到高价值目标时，其会针对该目标的内网情况进行重新研判，并挖掘内网常用软件 0day 漏洞进行更深层次的渗透。

从 2020 年海莲花组织整体攻击能力来看，其攻击能力开始逐渐向威胁等级三星的 APT 组织靠拢，隐藏攻击入口的能力大大增强，未来将更难发现该组织完整攻击链条。

第五章 APT活动的技术趋势

本章主要结合 2020 年奇安信威胁情报中心的 APT 活动监测与分析，给出当下流行的 APT 活动技术趋势分析。

一、0day、1day 与 APT 威胁

0day 漏洞一直是作为实施 APT 攻击的重要利器，无论是影子经纪人黑客组织泄露的方程式武器库中曝光的大量的 0day 漏洞利用装备，还是维基解密披露的 Vault7 项目中某西方大国情报机构用于管理的针对 Android 和 iOS 的漏洞利用列表文档，都展示了 0day 漏洞或成熟的漏洞利用链是实施网络攻击利用的关键能力。

我们整理了 2020 年用于在野攻击活动的 0day/1da y 漏洞列表（见表 5.1）。相较于 2019 年，2020 年被捕获的在野 0day 漏洞中并不存在严格意义上的文档类型漏洞，而针对浏览器的远程代码执行漏洞成为主流趋势，这一类的攻击中常常伴随着新的提权漏洞以用于浏览器沙盒逃逸。

值得注意的是，攻击者选用的漏洞目标逐渐从 Windows 下的原生浏览器，向 Chrome、Firefox 等用户量更大的浏览器转移，而受影响的也依旧集中在浏览器的脚本引擎上，如 Windows 下的 Jscript、Jscript9 及 Chrome 中的 V8。如果用一句话来总结 2020 年的在野 0day 利用情况，我们愿称之为“Chrome 漏洞利用年”。

表 5.1 列出了 2020 年，被 APT 组织利用最多的漏洞列表。

漏洞编号	影响目标	是否 0day	是否在野利用	相关组织
CVE-2019-17026	FireFox	是	是	Darkhotel
CVE-2020-0674	IE Jscript	是	是	Darkhotel
CVE-2020-0601	证书欺骗	否	是	未知
CVE-2020-6418	Chrome V8	是	是	未知
CVE-2020-8467	Apex One/OfficeScan	是	是	未知
CVE-2020-8468	Apex One/OfficeScan	是	是	未知

漏洞编号	影响目标	是否 0day	是否在野利用	相关组织
CVE-2020-0796	Windows SMB	否	是	未知
CVE-2020-6819	FireFox	是	是	未知
CVE-2020-6820	FireFox	是	是	未知
CVE-2020-0938	Windows 提权	是	是	未知
CVE-2020-1020	Windows 提权	是	是	未知
CVE-2020-1027	Windows 提权	是	是	未知
CVE 2020-12271	SQL 注入	是	是	未知
CVE-2020-0986	Windows 提权	是	是	未知
CVE 2020-15505	MobileIron	否	是	未知
CVE-2020-1380	IE Jscript9	是	是	未知
CVE-2020-0968	IE Jscript	否	是	多米诺行动
CVE-2020-1472	Windows	否	是	Muddy Wtaer
CVE-2020-15999	Chrome	是	是	未知
CVE-2020-17087	Windows 提权	是	是	未知
CVE-2020-16009	Chrome	是	是	未知
CVE-2020-16010	Chrome	是	是	未知
CVE-2020-27930	iOS	是	是	未知
CVE-2020-27950	iOS	是	是	未知
CVE-2020-27932	iOS	是	是	未知
CVE-2020-16013	Chrome	是	是	未知
CVE-2020-16017	Chrome	是	是	未知
CVE-2020-4006	VMware	是	是	未知

（一）DarkHotel 的 0day 漏洞在野利用

在面对高价值目标时，APT 组织会毅然决然地使用 0day 漏洞利用，而值得注意的是，一旦攻击组织使用 0day 漏洞作为攻击入口，那么其后续使用的提权漏洞同为 0day 漏洞的概率极高。

DarkHotel 就是一个长期使用浏览器类 0day 漏洞进行水坑攻击的 APT 组织。该组织通过入侵目标常用网站，将漏洞利用代码嵌入网站，当攻击目标访问网站后，通过判断目标的浏览器版本下发不同的漏洞利用代码，获取到初始权限后便会采取各种手段进行提权操作。

2020 年以来，该组织使用了多种浏览器 0day 漏洞发起攻击。下面我们将根据漏洞发现的时间线来依次展示：

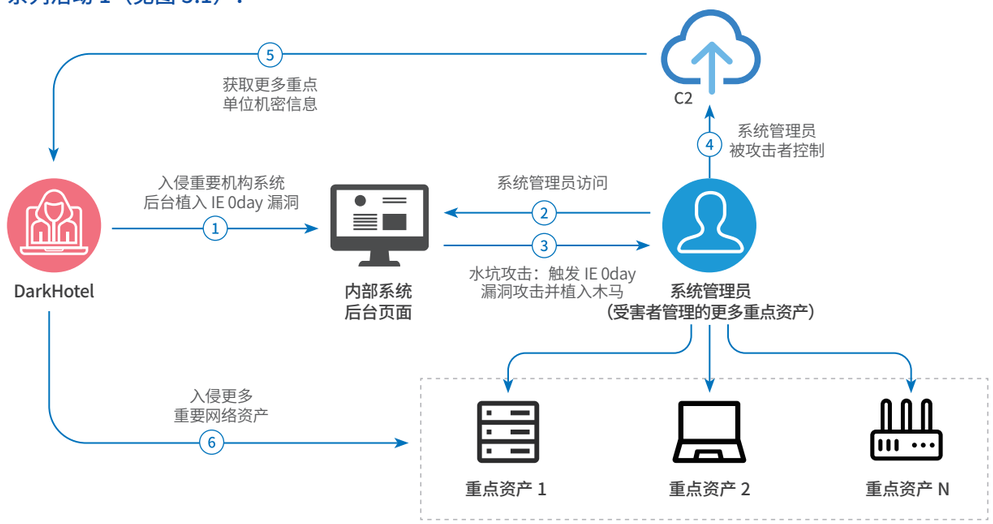
- 2020 年 2 月 6 日，利用两个浏览器的 0Day 漏洞（火狐浏览器：CVE-2019-17026；IE 浏览器：CVE-2020-0674）针对中国发起的 APT 攻击，过程中还涉及该组织以往拥有的 0day 漏洞武器：JavaScript 引擎 jscript.dll 中的漏洞 CVE-2019-1367、CVE-2019-1429、CVE-2019-0676、CVE-2018-8653 等。

- 2020 年 4 月，利用某 VPN 服务器 0day 漏洞针对中国机构进行攻击。

- 2020 年 5 月，发起 PowerFall 攻击活动，使用 IE 11 浏览器 JS 引擎的 jscript9.dll 的 0day 漏洞 CVE-2020-1380，并结合 Windows 权限提升漏洞 CVE-2020-0986 漏洞进行攻击。CVE-2020-0986 漏洞被认为是 CVE-2019-0880 漏洞的衍生版本。

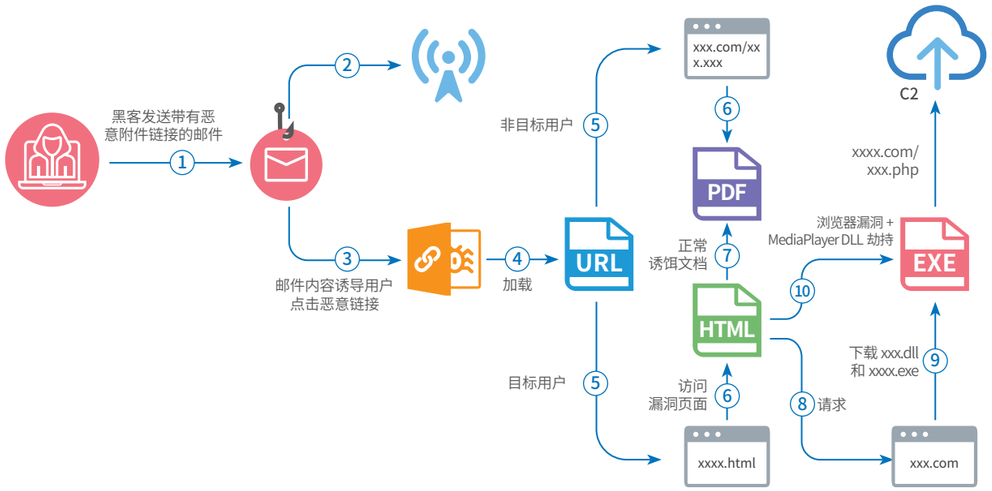
- 在 2020 年，奇安信红雨滴团队对 Darkhotel 利用多款浏览器漏洞的行为进行了监控，发现该组织针对多个国内重要机构的内部系统管理页面植入 0day 漏洞利用代码以执行水坑攻击，进而控制系统管理员的计算机以实施更广泛的入侵及横向移动。我们还原的整个攻击流程如下。

系列活动 1（见图 5.1）：



▲ 图 5.1 Darkhotel 组织针对国内重点机构网站植入 0day 漏洞代码

系列活动 2（见图 5.2）：



▲ 图 5.2 Darkhotel 组织利用我国某浏览器 0day 漏洞进行针对性的钓鱼攻击

而由于之后 CVE-2020-0674 EXP 的泄露，其被多个相关 APT 组织使用，如南亚响尾蛇组织通过投放恶意文档，运用模板注入的方式，结合 CVE-2017-0199 漏洞下载 hta 脚本，而该脚本还装载有 CVE-2020-0674 的漏洞利用代码，基于此进行了漏洞利用攻击。

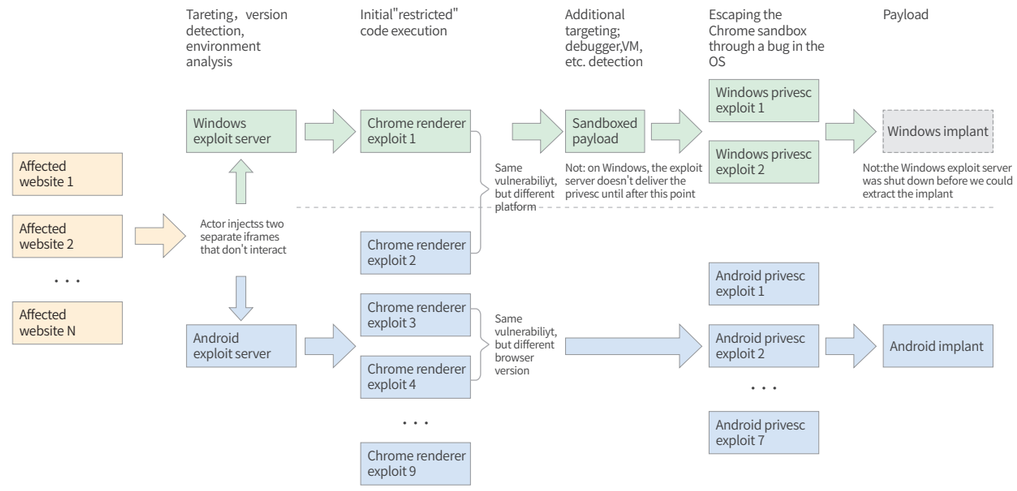
（二）不同产品的 0day 漏洞在野利用

值得注意的是，2020 年出现的在野 0day 漏洞攻击事件中，除了 Darkhotel 组织之外，其他攻击活动中均未确认明确的攻击归属。下面对其中一些重要的漏洞利用事件进行说明：

1）Chrome 浏览器 0day 漏洞在野利用

总共涉及 6 个相关被利用的在野 0day（CVE-2020-6418、CVE-2020-15999、CVE-2020-16009、CVE-2020-16010、CVE-2020-16013、CVE-2020-16017），大部分来自于 Google Project Zero 发现，也是 2020 年被在野利用最多的目标，但是具体的攻击背景未知。

这里值得一提的是 CVE-2020-6418，该漏洞在野利用由 Google Project Zero 发现，攻击者构造了多个用于水坑的 Web 页面，其针对的目标覆盖 Windows 及 Android 平台，通过 Chrome 漏洞获取执行权限，并通过 Windows/Android 的本地提权漏洞进行浏览器沙箱的逃逸，最终投递恶意代码。此处攻击活动中包括一个 Chrome 0day 漏洞 CVE-2020-6418，及三个 Windows 本地提权 0day 漏洞 CVE-2020-0938、CVE-2020-1020、 CVE-2020-1027，其具体的攻击流程如图 5.3 所示（引用 Google Project Zero 给出的攻击流程图）。



▲ 图 5.3 Google Project Zero CVE-2020-6418 攻击事件流程图

2）火狐浏览器 0day 漏洞在野利用

总共涉及两个相关被利用的在野 0day（CVE-2020-6819、CVE-2020-6820）。这两个漏洞由安全研究员 Francisco Alonso 及 Javier Marcos 发现，具体攻击细节未知。

3）苹果系统 0day 漏洞在野利用

总共涉及三个相关被利用的在野 0day（CVE-2020-27930、CVE-2020-27950、CVE-2020-27932）。这三个漏洞同样来在 Google Project Zero，具体的攻击者背景未知。

4）Windows 系统 0day 漏洞在野利用

总共涉及四个相关被利用的在野 0day（CVE-2020-0938、CVE-2020-1020、CVE-2020-1027、CVE-2020-17087）。

其中 CVE-2020-0938 由奇安信代码安全实验室及 Google 公司的 Project Zero and/ Threat Analysis Group 发现，另外三个由 Google Project Zero 发现。其中， Project Zero 证实，前三个漏洞被用于 CVE-2020-6418 在野 0day 的攻击事件中，以实现沙盒逃逸。

5）趋势科技披露的自家产品 0day 漏洞在野利用

趋势科技 Apex One 和 OfficeScan 在野 0day 漏洞（CVE-2020-8467、CVE-2020-8468），是趋势科技披露的自家相关产品漏洞，皆被用于在野攻击，具体攻击背景未知。

6）Sophos XG 防火墙 0day 漏洞在野利用

相关漏洞编号为 CVE 2020-12271。

7）VMware 0day 漏洞在野利用

VMware 命令注入漏洞（CVE-2020-4006）。美国 NSA 发布报告称，某具有国家背景的 APT 组织正在利用 VMware®1 Access 和 VMware Identity Manager2 产品中的漏洞，从而在原有权限的基础上提升到最高权限，从而可以执行任意命令。

（三）不同产品的 1day 漏洞利用

以下几个 1day 漏洞都属于 2020 年补丁修复后被披露，并被广泛使用。

Microsoft Exchange Control Panel (ECP) 漏洞 CVE-2020-0688，该漏洞由匿名人员提交给 ZDI，ZDI 于 2020 年二月补丁日微软修复之后披露了具体利用细节，并于之后被大量使用。

Zerologon（Windows CVE-2020-1472 漏洞），该漏洞由 Secura 于 2020 年 9 月补丁日修复后披露相关攻击细节：通过 Netlogon 远程协议 （MS-NRPC）建立与域控制器连接安全通道时，存在特权提升的利用点，该漏洞的 CVSS 分高达 10 分，攻击者只需要在内网中有一个立足点，就可以远程获取域控的管理员权限，并于之后被 MuddyWater 用于攻击活动之中。

IE JScript.dll 漏洞（Cve-2020-0968）：多米诺行动中，某俄语攻击组织通过 RTF 文档进行攻击。当文档被打开时，会自动进行远程网页加载，而加载的网页则内嵌了 CVE-2020-0968 的漏洞代码，基于此触发远程代码执行。

SMBGhost 漏洞（CVE-2020-0796）：在 Windows SMBv3 版本的客户端和服务端存在远程代码执行漏洞。由于该漏洞可以导致直接远程连接目标主机，因此被全球安全研究者进行分析，并且漏洞代码已经在地下黑市流通，用于攻击的组织持续至今。

Windows CryptoAPI 欺骗漏洞（CVE-2020-0601）：该 CryptoAPI 椭圆曲线密码（ECC）证书检测绕过漏洞由美国国家安全局（NSA）上报，在上报后被安全研究人员发现原理并进行方法公布，导致一些攻击者使用该欺骗方法进行程序数字签名绕过，从而利用进行攻击。

MobileIron 远程代码执行漏洞（CVE 2020-15505）：MobileIron 是移动设备管理（MDM）系统提供商，英国国家网络中心在 2020 年 11 月 23 日的通告中表示，APT 组织正在使用该漏洞攻击英国组织，美国网络安全和基础设施局（CISA）还指出，在一次 APT 组织入侵中，攻击者还结合 Netlogon / Zerologon 漏洞（CVE-2020-1472）进行利用。

二、移动终端场景 APT 威胁

针对智能手机是 APT 威胁的另一个威胁场景，其主要的目的在于实现监控和窃听，并针对特定的个人或群体。在以往的监测中，APT 活动在移动端通常会通过远程代码执行漏洞、钓鱼消息或者将间谍软件混入应用市场等方式在智能手机中植入后门程序，获取包括短信、通讯录、定位、文件、应用数据、录音和录像的数据。

2020 年，在移动终端场景方面，APT 组织依旧在各个渠道进行投放，诸如 Telegram、GooglePlay、iMessage 等，同时还出现了通过邮件投放的方式：例如邮件内嵌一张二维码，当受害者通过扫码后就会出现下载 APK 的提示。

2020 年，奇安信威胁情报中心对外披露了四个 APT 组织的移动端攻击活动，其中两个是奇安信威胁情报中心独立发现并率先命名的 APT 组织（诺崇狮组织和利刃鹰组织）。相关恶意软件主要以安卓端为主，但大部分代码的复杂度较低。

单一组织在移动端方面也会技术增强，2020 年南亚 APT 组织响尾蛇被发现利用 CVE-2019-2215 漏洞针对安卓终端目标用户实施移动 APT 攻击。

在移动端攻击领域还有一个霸主：以色列网络军火商 NSO Group，其于 2020 年售卖了多枚“核弹级”移动端应用的 0day 漏洞，其中包括在 WhatsApp、苹果 iMessage 中存在的 0day 漏洞。这些漏洞均被某些中东地区国家用于进行监视行动。

第六章 2021年高级持续性威胁预测

我们基于 2020 年 APT 威胁的趋势以及近年来 APT 威胁组织和活动的变化情况对 2021 年高级持续性威胁进行预测。

一、疫苗及相关产业将会遭到持续攻击

疫情贯穿了整个 2020 年，直到 2020 年末，全球已有 2000 多万人确诊新冠病毒，其中确诊人数趋势依旧呈上涨态势。这也就意味着，2021 年，疫情可能依旧会与全世界相伴。

2020 年，针对医疗卫生行业，特别是疾控部门和疫苗研制机构的 APT 活动已经成为年度焦点。显然，在 2021 年，这一趋势还将继续。特别地，2021 年将可能是人类历史上第一次全球疫苗大接种的一年，APT 组织很有可能也会针对疫苗研制、生产的相关机构发起持续性的网络攻击。同时，疫苗的相关产业，如疫苗流通（冷链设备、冷链运输、冷链流通和冷链物流等）、疫苗包装和原材料供应、疫苗终端使用和处理（注射器以及医疗废物处理等）等环节，都很有可能成为 APT 组织关注焦点。

二、针对中国的 APT 行动将持续加剧

中国作为 2020 年全球唯一实现经济正增长的主要经济体。面对世界百年未有之大变局，中国的经济与科技发展，正在经受着前所未有的巨大考验。

一方面，中国不断取得的技术突破使得我们在某些领域已经处于全球领先地位；另一方面，某些西方大国对部分中国科技企业采取持续的打压行动。这两个方面的形势，在 2020 年都有所加剧。这也就意味着，中国领先的科研机构、科技企业都将在 2021 年面临更加严峻、更加激烈的网络窃密活动与网络破坏活动。这也对中国政企机构的网络安全建设与运行水平提出了更高的要求。

三、远程办公各个环节都将遭受 APT 攻击

2020 年，在疫情的影响下，远程办公成为常态，而全球各地的 APT 组织也随之展开了大量针对远程办公软件或视频会议系统等的针对性网络攻击。

从目前的形势来看，疫情在 2021 相当长的时间里，仍然会在全球范围内广泛存在，远程办公的需求还会持续增长。因此，针对远程办公的 APT 活动也必将更加活跃。特别地，除了 VPN 和视频会议外，远程办公的其他各个相关环节都有可能成为 APT 攻击的突破口。

四、地区冲突将引爆更激烈的网络战

2020，APT 攻击活动仍与地区冲突紧密相关，西亚、中东等地区的政治、军事冲突，都引发了多起相关的 APT 活动。2021 年，如果地区冲突形势不能得到有效的缓解，那么地区冲突所带动的网络战活动也将随之愈演愈烈。

五、网络武器库的泄露或将常态化

自从 Shadowbroker 组织泄露方程式组织网络武器库开始，越来越多的民间黑客组织和政府支持黑客组织纷纷效仿这种泄露和窃取网络武器库的行为。

2020 年上半年，据称是某西方大国支持的黑客组织，入侵窃取并泄露了中东某国网军的武器库。2020 年末，火眼公司（FirEeye）的网络武器库也被攻击者窃取。这些事件都反映出一个共同的趋势：窃取其他国家或组织的网络武器库，可以给对敌方造成沉重的打击。

窃取了网络武器库后，攻击者不仅能提升自身的攻击水平，还可以更好地隐藏自己的身份。此外，利用他人的网络武器库进行入侵，也可以达成隐藏自己并嫁祸于他人的效果。

预计 2021 年，网络武器库依旧会存在泄露的风险，并且可能会不定期地曝光在大众视野中。而每次网络武器库的泄露，都有可能伴随这巨大全球性网络安全灾难发生。2015 年 7 月，意大利网络军火商 Hacking Team 武器库遭窃，导致次年全球网络挂马大流行；2017 年 3 月，APT 组织方程式的武器“永恒之蓝”被泄露，导致当年 5 月 WannaCry 病毒大流行，全球 100 多个国家的医疗、交通、工业企业及公共服务设施大面积瘫痪。

六、APT 组织可能组建基于 5G 与 IPv6 技术物联网僵尸网络

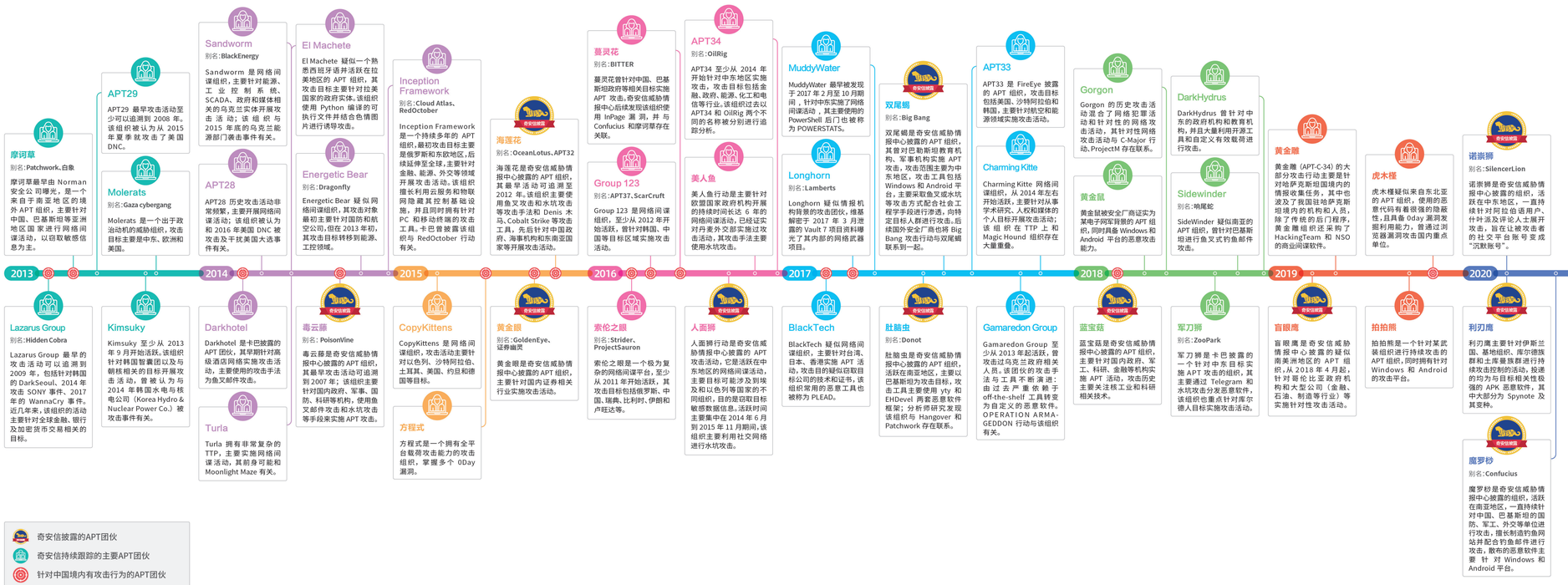
近年来，有多篇报告指出，APT 组织正在使用僵尸网络作为隐藏其网络资产的手段，例如，Lazarus 组织使用 tricbot 木马、APT28 组织使用 Dridex 和 VPNFilter 僵尸网络的资产作为 C&C 服务器发起攻击。

由于 5G 与 IPv6 技术的迅速普及和发展，已经有 APT 组织开始对其进行研究和尝试利用，这两种技术的结合利用点将有可能集中在僵尸网络攻击领域。

2021 年，随着 5G 与 IPv6 技术的进一步普及，APT 组织将有可能通过入侵大量使用了这些技术的智能家居或其他智能设备，从而组建大型物联网类僵尸网络进行攻击。而且，由于使用了 5G 技术，僵尸网络中被窃数据的回传速度将会提升到毫秒级。

附录1 全球主要APT组织列表

奇安信威胁情报中心 | 奇安信威胁情报中心持续跟踪
44 个主要 APT 团伙



附录2 奇安信威胁情报中心

威胁情报中心是奇安信集团旗下专注于威胁情报收集、分析、生产的专业部门，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威胁检测和大数据技术，依托亚太地区顶级的安全分析师团队，通过创新性的运营分析流程，开发威胁情报相关的产品和服务，输出威胁安全管理与防护所需的情报数据，协助客户发现、分析、处置高级威胁活动事件。

奇安信 ALPHA 威胁分析平台（https://ti.qianxin.com），是奇安信集团面向安全分析师和应急响应团队提供的一站式云端服务平台，该平台拥有海量互联网基础数据和威胁研判分析结果，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，提供全方位的威胁情报能力。

▼ 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3 红雨滴团队(Red Drip Team)

奇安信旗下的高级威胁研究团队红雨滴（RedDrip Team，@RedDrip7），成立于 2015 年（前身为天眼实验室），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 攻击组织的安全研究团队，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组织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 组织在中国境内的长期活动，并发布国内首个组织层面的 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

“红雨滴”背后的故事 — “从 100 亿个雨滴中找一个红雨滴”

2006 年 11 月 20 日，因发现 J 粒子而获得诺贝尔奖的著名华裔物理学家丁肇中教授来到中国驻瑞士大使馆，做了一场精彩的讲座。丁肇中教授形容自己发现构成物质的第四种基本粒子——J 粒子的高精度实验时说到：“相当于在北京下雨时，每秒钟有 100 亿个雨滴，如果有一个雨滴是红色的，我们就要从这 100 亿个里找出它来。”

而奇安信威胁情报中心高级威胁分析团队同样需要在海量数据中精准找寻那些红色威胁。最终，我们选择了“红雨滴”作为团队的名称。