2023-02

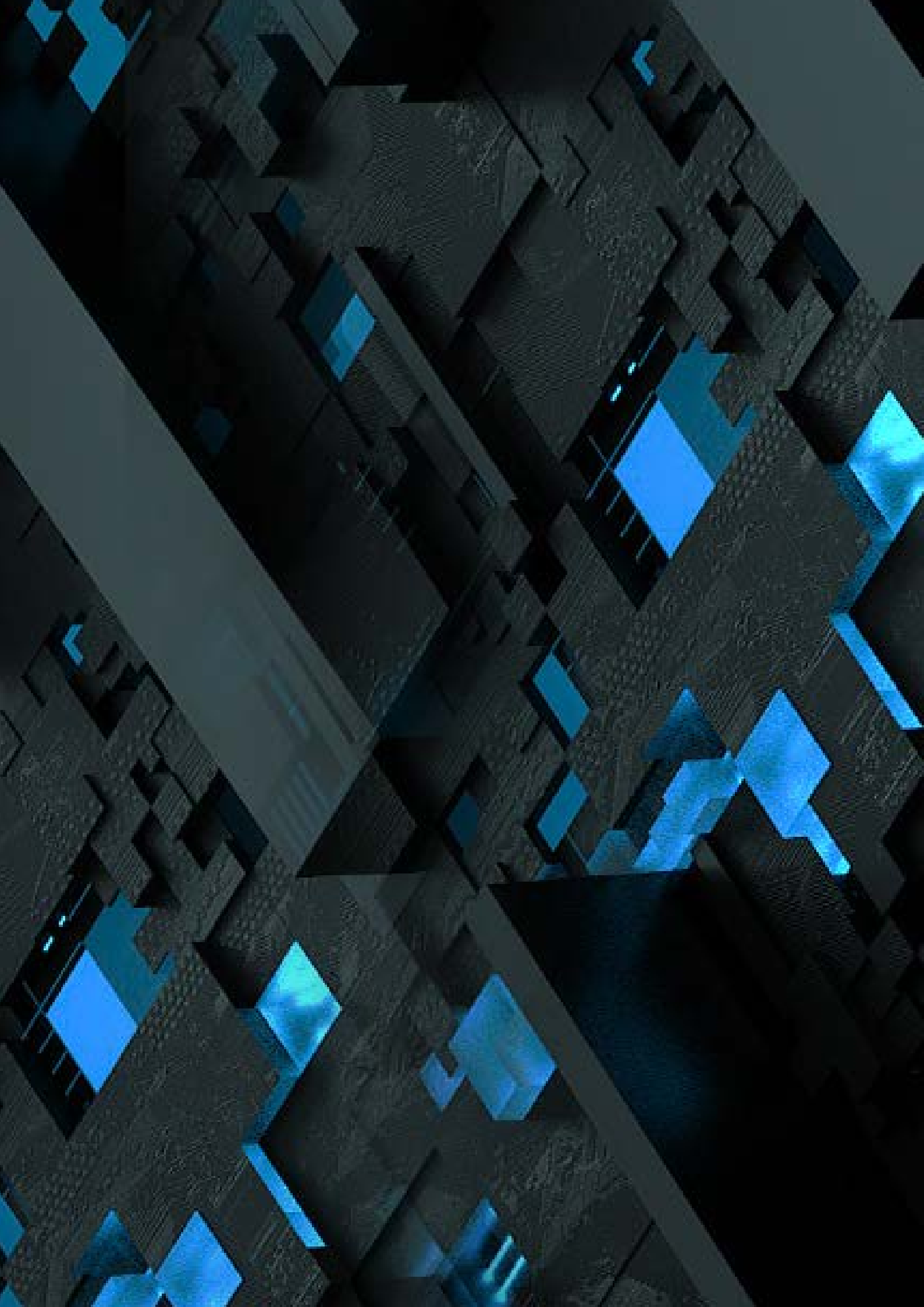
双子座实验室

天际友盟
TianJi Partners

2022 年下半年
全球主要 APT 攻击

活动报告

目录
CONTENTS



01 概述

2022 年下半年，天际友盟持续对 APT 组织及其活动进行追踪总结，总共披露了全球 98 个 APT 组织 160 多起攻击活动，通过对其中出现的威胁组织及其使用 TTP 的具体分析，我们总结出 2022 年下半年 APT 组织攻击活动特点如下：

1 地缘政治冲突不断激化，大国网络空间博弈加剧

持续近一年的俄乌战争并没有结束，其网络空间冲突也在不断升级。2022 年下半年，包括 Gamaredon、Sandworm、Trident Ursa、NoName057(16) 在内的俄罗斯黑客组织接连对乌克兰的政府、媒体、军队、供应商、电信公司、金融机构等组织发起攻击，而俄罗斯的政府、军队、外交等部门及其网站也遭受到了各方 APT 组织的猛烈攻击。虽然从披露的 APT 事件来看，俄罗斯方面似乎占据优势，但乌克兰凭借美国及其盟友的支持，也对俄罗斯发动了多起有影响的攻击，大国的网络空间博弈并未分出明显胜负。

2 网络间谍战硝烟弥漫，成为多国科技抗衡的有力手段

纵观世界，科技创新仍是发展的第一生产力，由此也衍生了不少旨在窃取机密资料的间谍组织。2022 年下半年，不仅有来自越南的海莲花组织、印度的白象等知名组织对我国政府、科研领域发起了网络间谍攻击，更有例如 APT-LY-1004 在内的新兴间谍组织在对印度国防部的钓鱼活动中浮出水面。从攻击手段来看，网络间谍人员擅长利用鱼叉式网络钓鱼策略针对与高新技术最接近的核心人员，可谓精准打击，出手果断。

3 美国超越乌克兰和俄罗斯，成为黑客组织攻击的热门目标

从攻击目标来看，美国成功超跃乌克兰，成为 2022 年下半年 APT 组织攻击最多的目标国家，其中来自俄罗斯和朝鲜的黑客组织贡献了超过一半的攻击。可见俄乌冲突对美国自身也有一定的影响。

4 软件行业漏洞频出，成为供应链攻击的主要切入点

从攻击行业来看，2022 年下半年软件行业已上升为除了政府和军工以外第三大易受黑客组织攻击的行业。由于软件行业巨头其产品分布广泛，借助他们产品或服务的漏洞进行传播或攻击的事件日渐增多，同时很多知名开源软件平台也成为供应链攻击的首选目标。

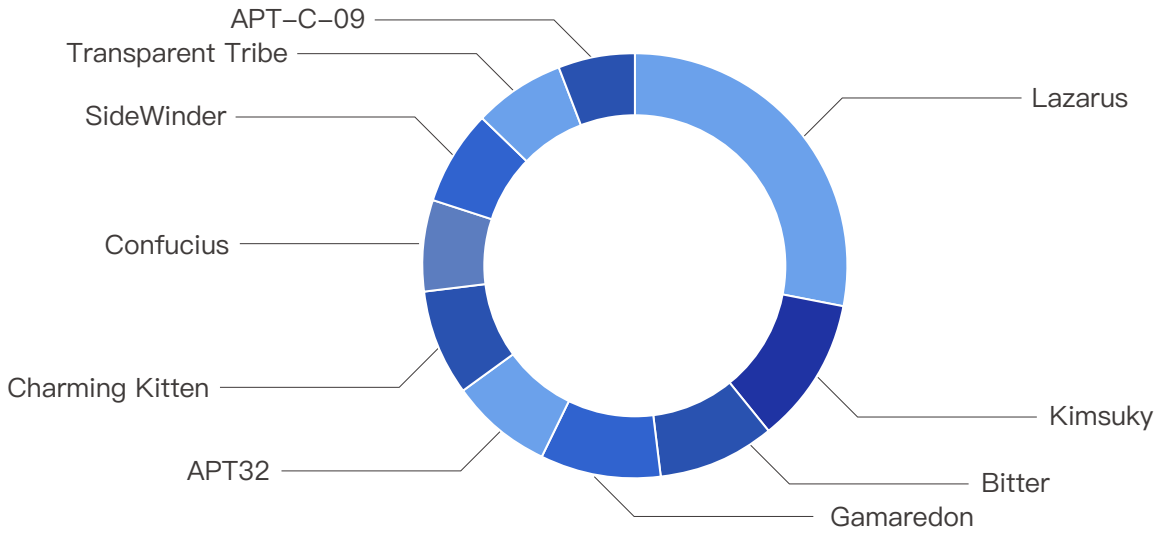
5 勒索软件攻击高度活跃，运营模式日渐成熟

从暗网活跃的几十个勒索软件团伙的数据披露网站可以看出，2022 年是勒索软件极为活跃的一年。其中，许多勒索软件正逐渐被黑客组织加入武器库，更有部分勒索软件团伙自身也发展壮大成新的威胁组织，他们有着成熟的运作模式并可对目标进行多重勒索。

02 APT 组织攻击数据披露

2.1 TOP 10 APT 组织

我们对 2022 下半年活跃的 TOP 10 APT 组织进行统计如下：

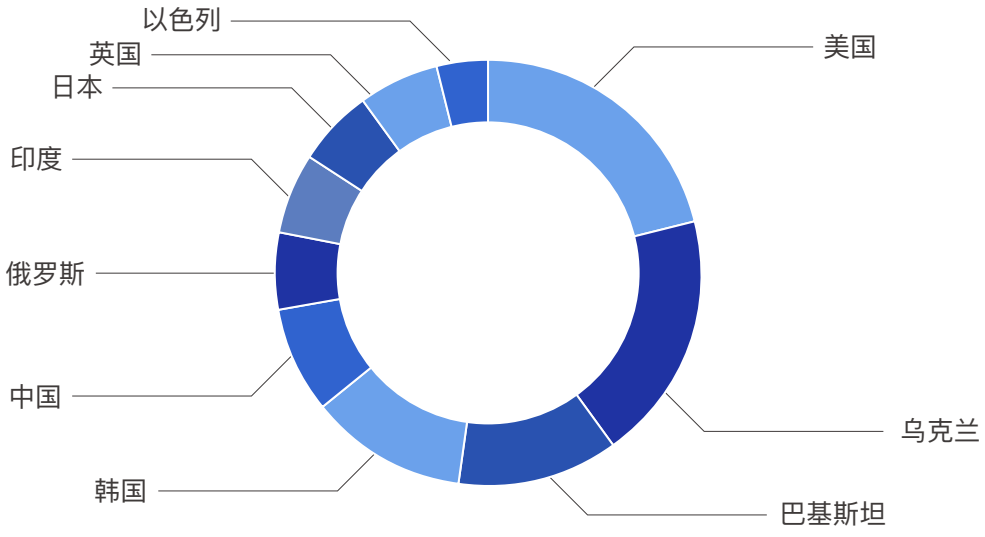


图表 1 2022 年下半年 TOP 10 APT 组织

2022 年下半年 160 多起攻击事件中（主要统计知名组织及有影响力的攻击），榜首依然被老牌黑客组织 Lazarus 占据，紧接着第二名是朝鲜黑客组织 Kimsuky，来自南亚的 APT 组织蔓灵花 BITTER 和俄罗斯黑客组织 Gamaredon 并列第三。 较 2022 年上半年而言，Kimsuky 组织上升最快，其攻击目标已扩展至 Android 设备。

2.2 TOP 10 攻击目标

2022 年下半年 APT 组织攻击的目标国家 TOP 10 统计如下：

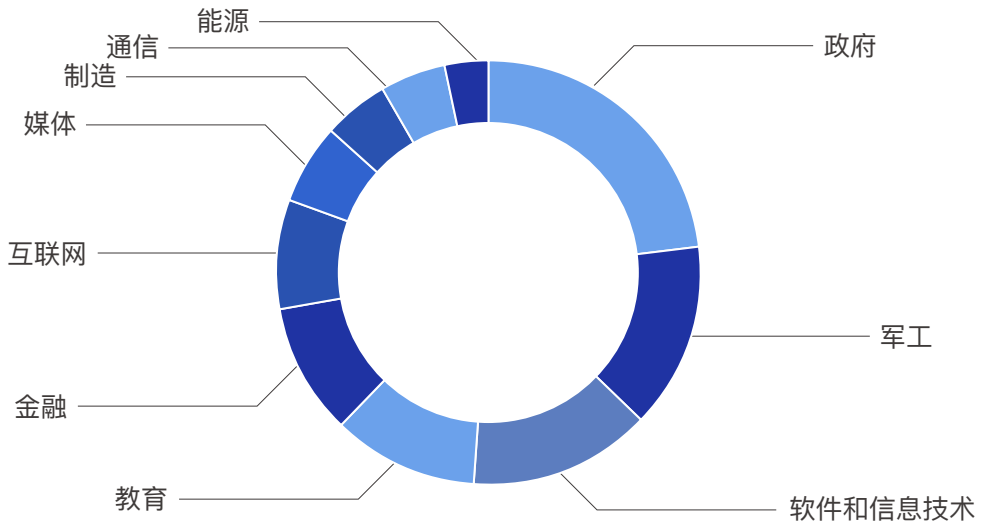


图表 2 2022 年下半年 TOP 10 APT 组织攻击目标

从统计数据可以看出，美国已经一跃成为 2022 年下半年以来黑客攻击目标的第一名，由于俄乌战争的影响，乌克兰紧随其后，巴基斯坦由于印度黑客组织的活跃攻击而位列第三名。

2.3 TOP 10 攻击行业

2022 年下半年 APT 组织攻击的目标行业 TOP 10 统计如下：

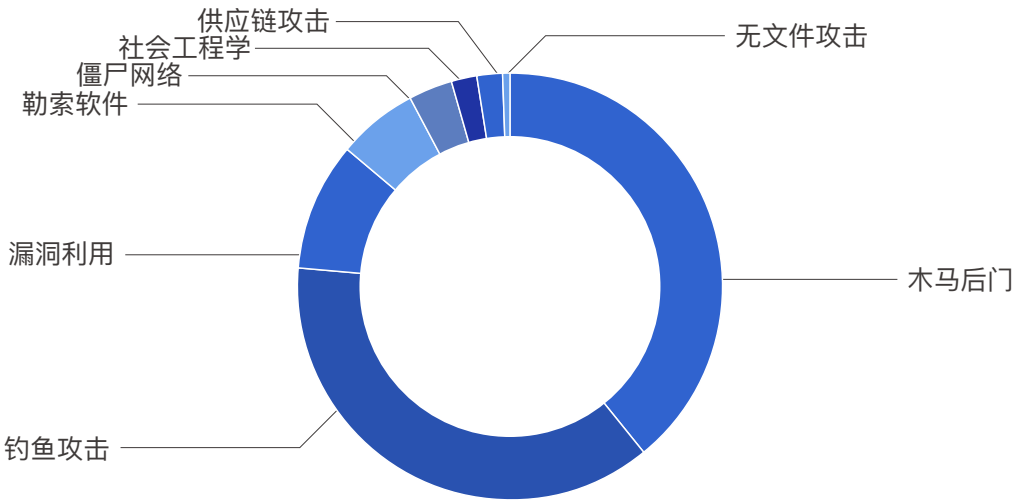


图表 3 2022 年下半年 APT 事件攻击行业分布 TOP 10

从上图可以看出政府、军工继续保持其热度，但软件和信息技术行业上升极快，已排到攻击目标行业的前三名，金融行业热度有所下降，已下滑到第 5 位。

2.4 APT 组织常见攻击手段

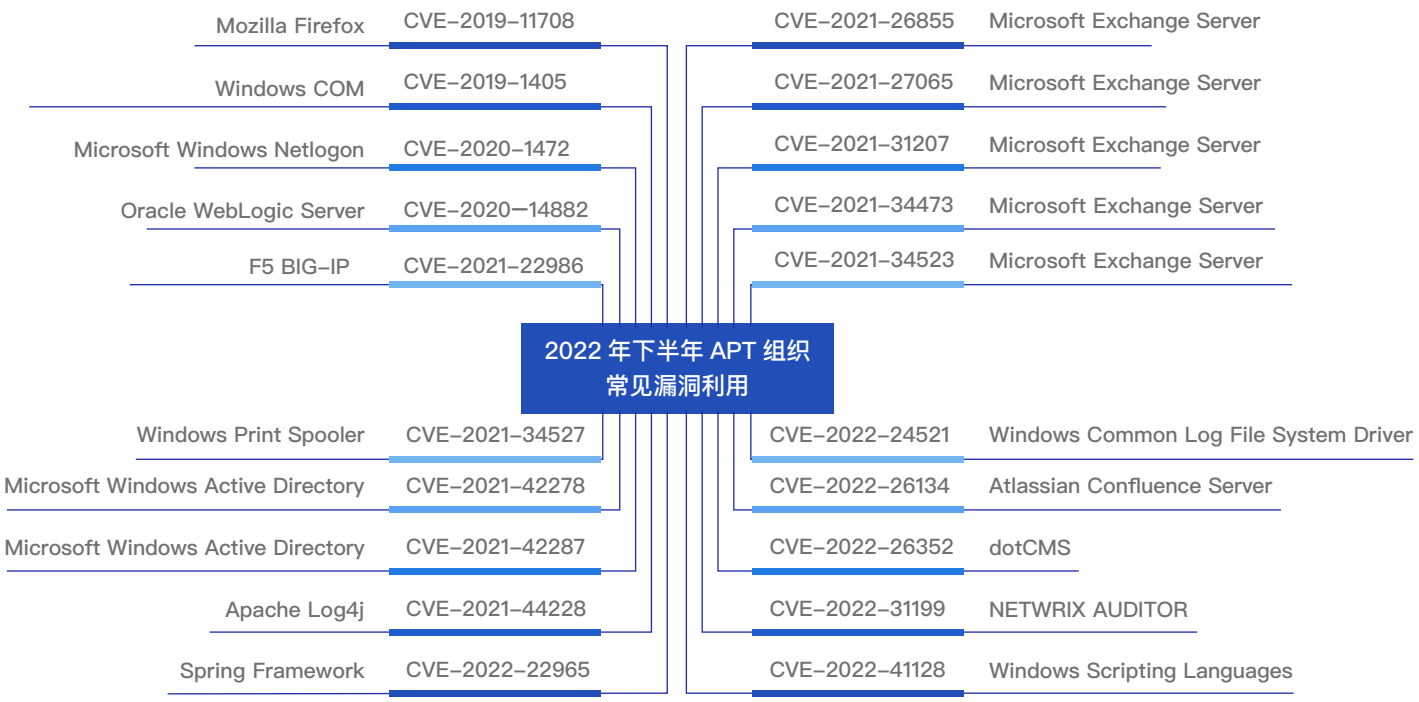
2022 年下半年 APT 组织常见攻击手段统计如下：



图表 4 2022 年下半年 APT 组织常见攻击手段

从表中可以看出，主要攻击手段的前三名依然被木马后门、钓鱼攻击、漏洞利用这三种手段占据。其中钓鱼攻击

中有三分之一的攻击活动使用了鱼叉式钓鱼攻击，用以提高攻击的成功率。漏洞利用作为初始渗透的有效手段，依然发挥着极其重要的作用。下表列出了 2022 年下半年最常用的漏洞列表及其针对的系统或软件：



图表 5 2022 年下半年 APT 组织常见漏洞利用

03 重大 APT 攻击活动

3.1 俄乌冲突相关攻击

俄乌冲突在 2022 年下半年局势持续紧张。俄乌双方依然频繁的遭受各类威胁组织和团伙的攻击。虽然从舆论战来看，乌克兰占据优势，但是俄罗斯凭借其强大的黑客能力，对乌克兰发起了多次有影响力的网络攻击。其中，俄罗斯 APT 组织 Gamaredon 及 Sandworm 是目前最为活跃的 APT 组织。来自俄罗斯的黑客组织 Gamaredon 一直以乌克兰为目标，并被认为对该国的数千起攻击负责。自 2022 年 2 月俄罗斯入侵以来，Gamaredon 针对乌克兰目标的活动已经发生了变化，涉及网络钓鱼攻击和部署新的恶意软件变体。

研究人员在 7 月份发现 APT 组织 Gamaredon 开始频繁使用多种不同类型的攻击方式对乌克兰赫尔松州、顿涅茨克州等地区的军方和警方目标进行网络攻击。在该攻击周期中，Gamaredon 主要使用了恶意 office 文档、html 附件、SFX 文件等攻击工具，配合其精心设计的诱饵信息，组合成了三类不同的攻击流程。在 2022 年 7 月 15 日至 8 月 8 日的一波攻击中，Gamaredon 使用最新的感染媒介涉及携带自解压 7-Zip 附件的网络钓鱼邮件，邮件中包含的 XML 文件导致执行 PowerShell 信息窃取程序。此外，Gamaredon 还会使用 VBS 下载器来获取 Pterodo 后门，该后门允许攻击者使用主机的麦克风录制音频，从桌面拍摄屏幕截图，记录和泄露击键内容，下载和执行其他 .exe 和 .dll 类型有效负载。9 月份，研究人员发现 Gamaredon 组织针对乌克兰开展了大规模的网络钓鱼活动，该活动旨在向乌克兰受害者主机分发信息窃取恶意软件 Infostealer，它可以泄露特定文件类型并在受感染端点上部署额外的二进制和

基于脚本的有效负载。

另一个知名俄罗斯黑客组织 Sandworm 也对乌克兰发起了相关攻击。2022 年 9 月份，Sandworm 组织使用伪装成乌克兰电信运营商的动态 DNS 域，对受害者网络发起鱼叉式网络钓鱼活动。Sandworm 使用独特的新基础设施，成功在关键的乌克兰系统上部署 Colibri Loader 和 Warzone RAT 恶意软件以传播其它恶意负载，这次攻击旨在支持俄罗斯地区的军事行动。11 月份，疑似 Sandworm 组织利用 RansomBoggs 新型勒索软件攻击乌克兰，新型勒索软件 RansomBoggs 基于 .NET 编写，一旦其进入受害者网络，将使用随机生成的密钥在 CBC 模式下使用 AES 算法加密文件，加密后文件扩展名更改为 .chsch。

除了 Gamaredon 和 Sandworm 两大组织以外，还有多个组织针对乌克兰的不同行业发起了攻击。

2022 年 6 月开始，研究人员调查并分析了用于对乌克兰境内及周边地区的网站进行 DDoS 攻击的恶意软件，确定该恶意软件是一种名为 Bobik 的 .NET 变体，包括一个 DDoS 模块，并通过僵尸网络传播。研究人员通过解密 HTTP 协议、监控 C2 服务器并收集有关定义 DDoS 目标的僵尸网络架构和 XML 配置的信息，确定了一个名为 NoName057(16) 的亲俄罗斯黑客组织。

7 月份 ITG23 组织针对乌克兰的攻击活动被披露，ITG23 是一个出于经济动机的网络犯罪团伙，主要以开发 Trickbot 银行木马而闻名，该木马于 2016 年首次被发现，从那时起，该组织就使用其有效载荷在勒索软件攻击的环境中站稳脚跟，包括 Ryuk、Conti 和 Diavol 勒索软件。数据盗窃或勒索软件的成功利用将为 ITG23 提供额外的勒索机会，特别是破坏性攻击可能会损害乌克兰的经济。同在 7 月，Malwarebytes 发现了黑客组织 UAC-0056(又名 UNC2589,TA471) 一系列针对乌克兰的网络攻击。此次活动该组织继续使用与之前相同的 TTP 针对乌克兰的政府实体。攻击活动的诱饵是基于与乌克兰正在发生的战争和人道主义灾难有关的重要文档，恶意文档会释放下一阶段的有效负载并最终部署 Cobalt Strike 有效载荷。

10 月份，新勒索软件 Prestige 被用于针对乌克兰、波兰运输和物流组织的持续攻击活动。该新勒索软件于 2022 年 10 月 11 日被首次发现在野使用，微软还发布了 Prestige 勒索软件部署的三种方法。成功部署后，Prestige 勒索软件有效负载将在其加密的每个驱动器的根目录中放置名为“README.txt”的勒索记录，且加密文件扩展名为 .enc。10 月 25 日乌克兰 CERT-UA 还发现 Tropical Scorpius 组织利用 RomCom 恶意软件攻击乌克兰。

11 月份，Blackberry 团队发现 RomCom 组织利用流行品牌软件包的欺诈活动，该活动主要针乌克兰和英国地区。11 月 15 日，俄罗斯黑客组织 FRwL（别称为 Z-Team、UAC-0118）使用 Somnia 勒索软件针对乌克兰的多个组织展开了网络攻击，并发布了针对乌克兰坦克生产商的攻击证据。

12 月份，俄罗斯 APT 组织 Trident Ursa 被曝出持续入侵乌克兰，Trident Ursa 依靠鱼叉式网络钓鱼策略以初步破坏目标设备，钓鱼诱饵包括 .html 文件和 Word 文档两种形式，并使用带有随机生成的变量名和字符串连接的 VBScript 来进行混淆。据报道该组织使用了许多合法工具和服务等技术提高其作战效率。12 月 21 日，Mandiant 发现了针对乌克兰政府的供应链攻击活动。活动由 UNC4166 组织发起，通过乌克兰语和俄语的 Torrent 文件共享网站分发伪装成合法 Windows 10 操作系统安装程序的木马化 ISO 文件，该恶意安装程序后续会投放进行侦察的恶意软件，并在一些受害者系统上部署工具以进行数据窃取。

2022 下半年发布的针对俄罗斯的 APT 攻击事件并不多，7 月份，Scarab APT、Mustang Panda 、Space Pirates、Tonto Team 等多个黑客组织使用 Royal Road 攻击了俄罗斯，攻击方式为使用钓鱼邮件来传递 Office 文档，最终下载精心选择的 RAT 恶意软件 Bisonal 等。11 月份 ，XDSpy 组织针对俄罗斯国防部发起钓鱼攻击，APT 组织 XDSpy 最早活跃于 2011 年，主要针对东欧和塞尔维亚地区的政府、军队、外交部及私人公司进行窃密活动。近期，该组织再次被发现利用 WSF 文件针对俄罗斯国防部开展钓鱼活动。

从披露的 APT 攻击事件来看，俄罗斯似乎占据优势，而实际的网络战争纷繁复杂，俄乌战争期间的大部分攻击集中在 DDOS 攻击上，APT 攻击占比不高，而且乌克兰背后还有美国和欧盟等国家的支持，所以这场网络空间大战的结果仍未分出明显胜负。

3.2 国内攻击情况

2022 年下半年，针对我国的攻击活动不在少数，且活动目标分布在政府部门、社会组织及科研院校中。与 2022 年上半年针对国内的攻击活动相比，攻击事件明显增加，且主要以信息窃取为目的。APT 组织不仅通过针对性的钓鱼邮件、僵尸网络等方式传播恶意软件，还新增了漏洞利用手段，攻击成功率大幅度上升。

8 月，国内研究人员发现活跃于越南的 APT32（海莲花）组织转向攻击我国关键基础设施单位，并且主要以窃取机密资料和重要文件为目标。经研判分析，海莲花组织的攻击方式多样，攻击链条复杂，但使用的核心攻击技术与最终木马载荷较为固定。在本次事件中，受害者为国家某关基单位研究员，APT32 组织采用鱼叉式网络钓鱼手段植入 RemyRAT 远程控制木马，靶向投递窃密程序以最终窃取关键研究资料及技术成果。

10 月，研究人员关注到了一个基于 Gafgyt 源代码开发并存在签名信息“daddyL33T's back”的僵尸网络木马。新型僵尸网络犯罪团伙 L33T 的命名便源于该签名信息。该团伙自 2021 年 9 月份开始就大规模布局，攻击范围涵盖了中国在内的 78 个国家和地区，攻击目标则包含了游戏、私服、教育网站等行业。其中，国内的广东、四川、以及中国香港、中国台湾等地均有受到影响。

来自印度的 APT-C-09（白象）组织最早于 2013 年曝光，其善于借助鱼叉式网络攻击手段投递有效载荷。国内研究人员同样在今年 10 月发现了来自该组织的攻击活动，APT-C-09 通过利用面向科研院所领域的诱饵文档投递其专用远控木马。文档伪造为某科学基金标题，并且包含 CVE-2017-11882 漏洞的利用条件。一旦该木马程序检测到受害主机的时区为中国，就会窃取受害者的数据并将其发送到攻击者的 C2 服务器。

11 月，趋势科技报道称 APT41 组织的新附属组织 Earth Longzhi 攻击目标已扩展至包括中国大陆、中国台湾地区在内的国防、航空、保险和城市发展等多个重要领域。

3.3 新兴威胁组织

随着恶意软件及服务的兴起，加之市场上存在大量可开源获取的工具，网络攻击的门槛及成本也随之降低。目前，已有越来越多的人参与网络犯罪，志同道合的黑客们更是组成了具有一定规模的组织。2022 下半年不仅存在新的专业 APT 组织活动，而且涌现了许多新型黑客团伙攻击事件。这些组织攻击手段及目标多样化，其中，电信和互联网提供商成为其重点攻击对象，更不乏有掺杂政治因素的俄乌对抗事件，对网络空间构成了更多不可预测的威胁。

8 月份，DeepWatch 安全中心披露新 APT 组织 TAC-040 利用漏洞 CVE-2022-26134 在 Confluence 服务器上执行代码，该组织还利用了 Spring4Shell 漏洞（CVE-2022-22965）来获得对 Confluence Web 应用程序的初始访问权限，之后更是在受害者的服务器上部署了一个名为 LjI 的新型永久后门。由于攻击者在入侵系统上部署了 XMRig 加密矿工，因此该组织极有可能以经济利益为目的。

9 月份，一个名为 Metador 的新黑客组织进入大众视野，该组织能够绕过 Windows 本地安全解决方案，同时可将包括 MetaMain 和 Mafalda 在内的恶意软件直接部署到内存中。Metador 组织目前主要针对中东和非洲几个国家的电信、互联网服务提供商和大学，且主要动机是开展间谍活动。

NoName057(16) 为一个亲俄的黑客组织，专注于 DDoS 攻击并寻找支持乌克兰或“反俄”的公司和组织，该组织

试图窃取数据或访问系统，攻击成功率在 40% 左右。9 月份，该组织被发现利用僵尸网络对属于乌克兰政府、新闻机构、军队、供应商、电信公司、运输当局、金融机构等组织的网站以及支持乌克兰的邻国（如爱沙尼亚、立陶宛、挪威、波兰）进行了 DDoS 攻击。

10 月份，SentinelLabs 报道一个名为 WIP19 的新威胁组织持续针对中东和亚洲的电信及 IT 服务提供商发起了攻击。WIP19 主要利用韩国公司 DEEPSoft 颁发的合法、被盗的数字证书来签署其新恶意软件，包括 SQLMaggie、ScreenCap 和凭证转储程序。

11 月初，研究人员捕获到了南亚地区“网络冲突间谍战”中的恶意文档文件，文件包含可最终加载文件窃密器的恶意宏代码。此次活动威胁组织主要针对印度国防部下设的 CSD 部门。11 月中旬，Abnormal Security 发现了一个疑似来自英国的新 BEC 组织 Crimson Kingsnake，攻击者主要通过冒充知名的律师事务所以欺骗会计专业人士支付虚假债务资金，其攻击目标遍及欧洲、中东、美国和澳大利亚等全球多个公司。

3.4 重点行业攻击

针对软件行业的攻击

2022 年下半年，软件行业一跃成为除政府、军工行业外第三大目标行业。黑客组织除了直接针对软件行业巨头公司以外（如 UNC2447 组织通过窃取思科员工的凭证开展攻击活动），大多数攻击利用了软件公司的产品或服务漏洞进行攻击，如 LV 组织利用 Microsoft Exchange 漏洞攻击约旦公司，Kimsuky 组织借助 IBM 公司的产品投递 BabyShark 恶意软件等，还有一些利用了大型开源软件或社区的软件包进行供应链攻击，如 APT 组织 ZINC 利用武器化开源软件针对多国进行攻击，CuteBoi 团伙利用 NPM 包进行大规模挖矿活动等。

针对教育行业的攻击

教育行业一直是 APT 组织攻击的热门目标，尤其是高校和科研机构。从 2022 的攻击事件来看，针对教育行业的攻击已超过金融行业，位列第四。除了勒索攻击以经济利益为目标外，很多针对科研机构的攻击都是以窃取科研成果，重要技术信息为目的。

2022 年下半年，朝鲜黑客组织 Lazarus 组织在 11 月份攻击了韩国的西江大学，采用模板注入方式下载恶意工具以窃取信息；印度白象组织 APT-C-09 利用 BADNEWS 远控木马攻击了中国的科研院校；Vice Society 组织利用多种勒索软件如 BlackCat、QuantumLocker 攻击全球（尤其为美国）教育行业；活跃于南亚的 APT 组织 Patchwork 从去年开始针对多国科研目标进行了一系列渗透攻击活动。

针对金融行业的攻击

随着 APT 组织攻击范围的逐步扩大以及 TTP 的不断演化，其攻击活动波及的行业也越来越广泛。之前，金融业作为传统的最容易获取经济利益的行业，一直是 APT 组织热门的攻击目标，但是在 2022 年下半年针对金融行业的攻击比重却有所下降。

老牌黑客组织 Lazarus 组织继续调整目标行业，不只针对韩国地区的金融行业，也瞄准了日本瑞穗銀行求职人员，另外还通过使用 DTrack 后门攻击欧洲和拉丁美洲的多个国家，同时 Lazarus 在加密货币领域的攻击也颇为频繁。

APT 组织 TA505（别名 Evil Corp、Gold Drake、Dudear、Indrik Spider 和 SectorJ04）是一个俄罗斯网络犯罪集团，近年来与许多勒索软件活动有关。9 月份，该组织使用名为 TeslaGun 的控制面板来操纵 ServHelper 后门，并作为 C2 来控制受感染的机器。Proofpoint 研究人员在下半年还发现 TA4563 黑客组织利用 Evilnum 恶意软件攻击欧洲金融和投资实体的恶意活动，尤其针对那些支持外汇、加密货币和去中心化金融的业务实体。

3.5 勒索软件攻击

由于不仅存在专注于获取经济利益的勒索团伙及其附属机构，并且越来越多的黑客乃至专业的 APT 组织都开始使用勒索软件以实现简单高效的数据盗取目的，勒索软件在 2022 年下半年依然保持着极高的网络攻击市场占有率。

7 月，朝鲜黑客组织 DEV-0530 被发现利用 H0lyGh0st 勒索软件攻击中小型企业。该组织主要为实现财务目标而开展勒索活动，并通过暗网站点与受害者进行交易。但是，DEV-0530 采用了更具压迫的勒索策略，其威胁受害者称，将在社交媒体上发布所窃取的数据或者将直接发送给受害者的客户。此外，该组织似乎与朝鲜知名 APT 组织 Lazarus 存在明显关联，两者不仅在同一基础设施集上运行，甚至还使用了名称相似的自定义恶意软件控制器。

激进的俄罗斯网络犯罪集团 TA505，近年来与许多勒索软件活动有关。9 月份，该组织开始利用名为 TeslaGun 的控制面板来操纵 ServHelper 后门，并作为 C2 来控制受感染的机器。除了使用面板外，攻击者还通过远程桌面协议 (RDP) 会话下载和安装定制的恶意工具。目前，该组织已通过针对性网络钓鱼活动攻击了至少 8160 个目标，且大多数受害者位于美国、俄罗斯、巴西、罗马尼亚和英国。

10 月可谓是勒索活动爆发期，其中与 LockBit 相关的勒索活动更是屡见不鲜，LockBit 3.0 勒索软件于 2022 年 7 月正式推出，并于 10 月初被攻击者包装为 NSIS 和 Word 文档格式的求职申请钓鱼邮件进行分发。中旬，由 DEV-0960 组织运营的新勒索软件 Prestige 横空出世，其通过多种部署方法用于持续针对乌克兰、波兰的运输和物流组织。月末，Microsoft Exchange 服务器成为攻击者的主要入口点。首先，BlackByte 附属机构被发现利用 ProxyShell 和 ProxyLogon 漏洞入侵 Microsoft Exchange 服务器，并开始使用基于 Go 语言编写的自定义数据泄露工具 Infostealer.Exbyte 加快其窃取和渗出数据的速度。其次，疑似源于 REvil 组织的 LV 组织也被观察到利用 Microsoft Exchange 服务器漏洞攻击约旦公司。目前，该组织的受害者多位于欧洲地区，其中，美国、沙特阿拉伯受攻击尤其明显，且主要受影响行业为制造业和技术相关行业。同样在此期间，Daixin Team 勒索组织袭击了美国医疗保健和公共卫生 (HPH) 部门，并通过窃取用户个人身份信息 (PII) 和受保护的健康信息 (PHI) 以威胁受害者支付赎金。

Vice Society 勒索团伙为机会主义攻击者，目前没有明显的地域重点。目标是中小型企业，并因针对教育部门而臭名昭著，其在今年 7 月至 10 月期间也依旧保持着对学校组织的高调攻击姿态。

Black Basta 于 2022 年 4 月首次出现，攻击目标涉及美国、加拿大、英国、澳大利亚和新西兰等，截止 2022 年 9 月已入侵 90 多个组织。11 月，该组织再次被发现通过钓鱼邮件投放 QBot 恶意软件 (也称为 QakBot、Pinkslipbot）针对美国公司开展了广泛的勒索攻击活动。此外，该勒索团伙被报道疑似与 FIN7 组织存在一定关联。FIN7 是一个出于经济动机的黑客组织，自 2012 年以来一直活跃。最初，FIN7 使用 POS 恶意软件进行金融欺诈，但自 2020 年以来，其转向开展勒索软件业务。

12 月份，与多个威胁组织（例如 Silence、TA505）存在关联的恶意软件 TrueBot 攻击活动被报道传播了 Clop 勒索软件。该活动攻击者最初主要使用恶意电子邮件作为初始入侵方式。但是在八月份，攻击者开始尝试利用 Netwrix 审计器中的远程代码执行漏洞 CVE-2022-31199。10 月份，Raspberry Robin（一种通过 USB 驱动器传播的恶意软件）再次变化为其主要传递媒介。

04 总结

纵观 2022 年，随着俄乌战争的发展，地缘政治冲突导致的 APT 攻击事件仍然占主导地位，政治、军事目标依然是国家级黑客组织攻击的重要标地。预计 2023 年，虽然国际政治局势有可能缓和，但是地缘政治冲突背后的大国博弈依然暗潮汹涌，政府、军工必将还是黑客组织争夺的攻击目标。相比于 2021 年，2022 年金融行业的攻击占比有所下降，但教育、软件、医疗、能源、工控、云服务等行业的攻击却不断增多，说明黑客组织的攻击格局已经全面打开，向着越来越广泛的行业和目标发展。

以经济利益为根本动机的勒索软件组织或团伙近年来得到飞速发展，其业务模式已形成一定规模，并逐步进入成熟发展阶段。2022 年多个大型勒索软件组织或团伙如 LockBit、Cuba、 BlackCat、BianLian 等频繁在暗网上发布其盗取的公司数据，并公然索要赎金。同时由于勒索软件 RaaS 模式的盛行，加之附属组织的积极推广，又涌现出很多中小型勒索团伙。勒索软件的肆虐发展，已经对全球产业造成了巨大的经济损失，预计在 2023 年，这一势头仍将扩大。

综上所述，从 2022 年全年来看，地缘政治、经济利益仍是网络攻击的根本动机，以钓鱼仿冒技术为切入点，以漏洞利用或木马后门为攻击手段的 APT 攻击事件增长迅速。天际友盟提醒网络安全人员采取针对性措施，及时部署防御、检测和响应方案，以应对日益严重的网络威胁环境。

05 附录

2022 年下半年 APT 组织活动时间表：

时间	APT 事件	组织名称	攻击行业
12 月 30 日	疑似 Kimsuky 组织冒充韩国知名网站 Naver 发起钓鱼攻击	Kimsuky	金融
12 月 30 日	RedDelta 组织持续迭代 PlugX 后门入侵欧洲政府	Mustang Panda	政府
12 月 30 日	CNC 组织利用摆渡木马针对军工和教育行业	CNC	军工、教育
12 月 29 日	Lazarus 组织针对加密货币和 NFT 用户开展大规模钓鱼活动	Lazarus	互联网
12 月 29 日	巴基斯坦 IBO 反恐部队遭遇印度组织 Confucius 网络攻击	Confucius	军工、政府
12 月 28 日	BlueNoroff 组织引入绕过 Windows MotW 保护新方法	APT38	金融
12 月 28 日	针对哥伦比亚的盲眼鹰组织近期攻击活动剖析	APT-C-36	政府、金融

时间	APT 事件	组织名称	攻击行业
12 月 27 日	Lazarus 组织利用经证书签名的恶意软件攻击 macOS 用户	Lazarus	互联网
12 月 26 日	APT 组织 SideCopy 瞄准印度政府官员	SideCopy	政府
12 月 26 日	黑客组织 Eternity 详情披露	Eternity	
12 月 26 日	双尾蝎组织新型移动端恶意软件揭秘	APT-C-23	互联网
12 月 23 日	FIN7 组织创建自动攻击平台 Checkmarks 破坏 Exchange 服务器	FIN7	软件和信息技术
12 月 22 日	俄罗斯 APT 组织 Trident Ursa 持续入侵乌克兰	Gamaredon	能源
12 月 21 日	UNC4166 组织利用木马化的 Win10 操作系统安装程序瞄准乌克兰政府	UNC4166	政府
12 月 19 日	MCCrash 僵尸网络对私人 Minecraft 服务器发起 DDos 攻击	DEV-1028	软件和信息技术
12 月 19 日	MirrorFace 组织针对日本政治实体开展 LiberalFace 活动	MirrorFace	政府
12 月 16 日	Royal 勒索软件组织剖析	Royal	医疗
12 月 16 日	响尾蛇组织近期瞄准巴基斯坦学校及军队	SideWinder	军工、教育
12 月 14 日	伊朗间谍组织 APT42 及关联 APT 追踪	Charming Kitten	军工、媒体、教育、社会组织、制造、医疗
12 月 13 日	恶意软件 TrueBot 攻击活动，传播新窃密工具和 Clop 勒索软件	Silence、TA505	金融、教育
12 月 12 日	DeathStalker 组织利用 Janicab 木马新变种攻击律师事务所	DeathStalker	服务业
12 月 12 日	伊朗组织 MuddyWater 针对亚洲和中东国家发起钓鱼攻击	MuddyWater	服务业、金融
12 月 9 日	Callisto 组织瞄准支持乌克兰的实体	Calisto	社会组织、教育
12 月 9 日	俄罗斯组织 TAG-53 针对美国军事企业发起钓鱼攻击	TAG-53	军工
12 月 9 日	伊朗 APT 组织 Agrius 通过供应链攻击部署 Fantasy 擦除器	Agrius	软件和信息技术、制造
12 月 8 日	TeamTNT 挖矿组织剖析	TeamTNT	软件和信息技术
12 月 8 日	朝鲜 APT37 组织利用 IE 0-day 漏洞袭击韩国	APT37	软件和信息技术
12 月 7 日	Vice Society 勒索团伙详情披露	Vice Society	教育、医疗、社会组织
12 月 7 日	疑似 APT-C-56 瞄准巴基斯坦恐怖主义分子	Transparent Tribe	社会组织
12 月 6 日	Cranefly 组织使用新技术从合法 IIS 日志中读取命令	UNC3524	软件和信息技术
12 月 5 日	黑客组织 Lazarus 利用 AppleJeus 变种软件继续针对加密货币用户	Lazarus	互联网
12 月 5 日	海莲花组织利用 Torii 远控木马针对物联网设备	APT32	软件和信息技术
12 月 2 日	UNC4191 组织利用 USB 驱动器开展间谍活动	UNC4191	软件和信息技术
12 月 1 日	CashRewindo 组织使用老化域名进行恶意广告活动	CashRewindo	互联网

时间	APT 事件	组织名称	攻击行业
12 月 1 日	ScarCruft 组织武器库扩充 Dolphin 后门	APT37	软件和信息技术
11 月 30 日	Kimsuky 组织借助 IBM 公司产品投递 BabyShark 恶意软件	Kimsuky	软件和信息技术
11 月 30 日	Lazarus 组织瞄准日本瑞穗銀行求职人员	Lazarus	金融
11 月 29 日	疑似 Sandworm 组织利用 RansomBoggs 勒索软件攻击乌克兰	Sandworm	
11 月 28 日	OPERA1ER 组织攻击非洲银行和金融机构	OPERA1ER	金融
11 月 25 日	Bahamut 组织利用虚假 VPN 程序欺骗 Android 用户	Bahamut	互联网
11 月 24 日	Black Basta 组织使用 QBot 恶意软件攻击美国公司	Black Basta	金融
11 月 24 日	摩诃草组织再次袭击巴基斯坦	APT-C-09	政府
11 月 23 日	WatchDog 黑客组织持续瞄准东亚云服务商	WatchDog	通信
11 月 22 日	Kasablanka 组织 LodaRAT 恶意软件分析	Kasablanka	
11 月 22 日	疑似中东某国情报部门针对也门开展间谍活动	Kasablanka	媒体
11 月 21 日	APT 组织 Mustang Panda 详情披露	Mustang Panda	政府
11 月 18 日	伊朗黑客利用 Log4Shell 漏洞入侵美国政府组织		政府
11 月 17 日	Billbug 组织袭击亚洲政府和证书颁发机构	Lotus Blossom	政府、软件和信息技术
11 月 16 日	Lazarus 组织持续使用 DTrack 后门攻击多个国家	Lazarus	软件和信息技术、教育、通信、金融、政府、制造
11 月 16 日	XDSpy 组织针对俄罗斯国防部发起钓鱼攻击	XDSpy	军工
11 月 15 日	APT 组织海莲花内网渗透手法详情披露	APT32	软件和信息技术
11 月 15 日	俄罗斯组织 FRwL 利用 Somnia 勒索软件瞄准乌克兰	FRwL	软件和信息技术
11 月 14 日	Worok 黑客组织在 PNG 文件中隐藏 DropBoxControl 后门	Worok	政府、能源
11 月 11 日	Keksec 组织利用 Cloud9 恶意浏览器扩展窃取用户信息	Keksec	软件和信息技术
11 月 10 日	APT41 新附属组织 Earth Longzhi 详情披露	Earth Longzhi	金融、公共设施、航空航天、军工、医疗、政府
11 月 9 日	疑似 FIN7 组织与 Black Basta 勒索团伙存在关联	FIN7、Black Basta	金融
11 月 9 日	Crimson Kingsnake 组织冒充律师事务所攻击全球公司	Crimson Kingsnake	服务业
11 月 9 日	金刚象组织利用虚假社交应用攻击巴基斯坦军方	VajraEleph	军工
11 月 8 日	APT 组织蔓灵花近期活动样本分析	BITTER	能源、军工、政府
11 月 7 日	Transparent Tribe 组织利用新 TTP 和工具瞄准印度政府	Transparent Tribe	政府

时间	APT 事件	组织名称	攻击行业
11 月 4 日	RomCom 组织利用流行软件包攻击乌克兰、英国	RomCom	软件和信息技术
11 月 3 日	黑产团伙模仿 Lazarus 组织攻击手法		金融
11 月 2 日	APT-LY-1004 针对印度国防部开展持久间谍活动	APT-LY-1004	军工
11 月 2 日	朝鲜 Lazarus 组织持续攻击韩国地区	Lazarus	教育
11 月 2 日	BRONZE PRESIDENT 组织针对政府官员发起钓鱼攻击	BRONZE PRESIDENT	政府
11 月 1 日	APT10 组织 LODEINFO 恶意软件演变追踪	APT10	
10 月 31 日	UNC3524 组织利用新 dropper 程序秘密收集情报	UNC3524	
10 月 31 日	疑似 TeamTNT 组织发起 Kiss-a-dog 挖矿活动	TeamTNT	软件和信息技术
10 月 28 日	印度白象组织利用 BADNEWS 木马攻击中国科研院校	APT-C-09	教育
10 月 28 日	Vice Society 组织利用多种勒索软件攻击教育部门	Vice Society	教育
10 月 27 日	Kimsuky 组织针对 Android 设备的新恶意软件分析	Kimsuky	互联网
10 月 27 日	PatchWork 组织 Herbminister 行动武器库披露	APT-C-09	教育
10 月 26 日	LV 组织利用 Microsoft Exchange 攻击约旦公司	LV	软件和信息技术、制造
10 月 26 日	Daixin Team 勒索组织瞄准美国卫生部门	Daixin Team	医疗
10 月 25 日	UAC-0132 组织利用 RomCom 恶意软件攻击乌克兰	Tropical Scorpius	军工
10 月 24 日	APT 组织 SideWinder 利用 WarHawk 后门攻击巴基斯坦	SideWinder	军工、政府
10 月 24 日	BlackByte 勒索软件活动部署新渗透工具 Exbyte	Hecamede	软件和信息技术
10 月 21 日	APT-C-50 组织利用 FurBall 间谍软件监视伊朗公民	Domestic Kitten	互联网
10 月 21 日	新型僵尸网络犯罪团伙 L33T 详情披露	L33T	教育、互联网
10 月 20 日	TeamTNT 组织疑似卷土重来	TeamTNT	软件和信息技术
10 月 20 日	APT 组织海莲花近期攻击活动分析	APT32	服务业、媒体、政府、制造
10 月 19 日	DiceyF 组织利用 GamePlayerFramework 攻击在线赌场	DiceyF	娱乐
10 月 18 日	新间谍组织 WIP19 瞄准电信及 IT 服务提供商	WIP19	通信
10 月 17 日	Budworm 间谍组织近 6 月活动跟踪	APT27	医疗、政府、制造
10 月 17 日	新勒索软件 Prestige 攻击乌克兰、波兰组织	DEV-0960	交通
10 月 12 日	LockBit 3.0 勒索软件伪装成求职申请进行分发	LockBit	

时间	APT 事件	组织名称	攻击行业
10 月 12 日	针对以色列的 POLONIUM 组织工具集详情披露	POLONIUM	通信、软件和信息技术、服务业、金融、媒体
10 月 10 日	LofyGang 分发大量恶意 NPM 包窃取信用卡信息	LofyGang	互联网
10 月 9 日	APT 组织 ZINC 利用武器化开源软件针对多国发起攻击	Lazarus	软件和信息技术、航空航天、军工、媒体
10 月 9 日	Water Labbu 组织利用 Cobalt Strike 感染 MeiQia 程序	Water Labbu	互联网
10 月 8 日	DeftTorero 组织详情披露	DeftTorero	教育、军工、通信、媒体、政府
10 月 8 日	Eternity 在暗网中出售 LilithBot 恶意软件	Eternity	软件和信息技术
9 月 30 日	Lazarus 组织针对加密货币领域开展钓鱼活动	Lazarus	互联网
9 月 29 日	俄罗斯组织 APT28 利用 PowerPoint 传播 Graphite 恶意软件	APT28	军工、政府
9 月 27 日	Lazarus 组织利用 BYOVD 再次攻击韩国	Lazarus	军工、金融、媒体
9 月 27 日	Void Balaur 网络雇佣军组织详情披露	Void Balaur	金融、服务业、政府
9 月 26 日	新 APT 组织 Metador 攻击电信、互联网服务和大学	Metador	通信、互联网、教育
9 月 26 日	Scarlet Mimic 组织长期监控维吾尔族社区	Scarlet Mimic	社会组织
9 月 23 日	APT 组织 TA413 利用自制后门持续针对藏族社区	TA413	社会组织
9 月 22 日	APT 组织 UAC-0113 伪装成电信公司瞄准乌克兰	Sandworm	通信、政府
9 月 21 日	响尾蛇组织最新活动追踪	SideWinder	
9 月 19 日	UNC4034 组织利用 WhatsApp 传播恶意软件	UNC4034	媒体
9 月 16 日	APT 组织 Gamaredon 针对乌克兰政府开展间谍攻击	Gamaredon	政府
9 月 15 日	APT 组织 TA453 利用多角色模拟新技术发起钓鱼攻击	Charming Kitten	能源
9 月 14 日	Kimsuky 组织再次针对韩国发起突袭攻击	Kimsuky	政府
9 月 13 日	APT 组织 Lazarus 利用 MagicRAT 控制受害者网络	Lazarus	软件和信息技术
9 月 9 日	新伊朗黑客组织 APT42 详情披露	Charming Kitten	教育、媒体、政府
9 月 9 日	TA505 黑客利用 TeslaGun 面板操纵 ServHelper 恶意软件	TA505	服务业、互联网、金融
9 月 9 日	新网络间谍组织 Worok 攻击亚洲公司和政府	Worok	政府
9 月 9 日	NoName057(16) 组织通过 DDoS 攻击瞄准乌克兰支持者		媒体、通信、军工、金融、政府、制造
9 月 5 日	Lilith 僵尸网络及 Jester 黑客团伙跟踪	Eternity	软件和信息技术

时间	APT 事件	组织名称	攻击行业
9 月 2 日	APT 组织 Evilnum 再次针对在线交易开展网络攻击	Evilnum	互联网
9 月 1 日	TA423 利用 ScanBox 框架开展间谍活动	APT40	制造、能源
8 月 31 日	Bahamut 组织利用 AndroidRAT 新变种窃取用户信息	Bahamut	
8 月 30 日	APT-C-08 最新远控组件 wmRAT 分析	BITTER	军工、外交机构、政府、教育
8 月 30 日	MERCURY 组织利用 Log4j 2 漏洞攻击以色列组织	MuddyWater	
8 月 29 日	朝鲜 APT 组织 Kimsuky 攻击韩国媒体和智库	Kimsuky	教育、政府、媒体、外交机构
8 月 25 日	APT 组织 Charming Kitten 新数据窃取工具详情披露	Charming Kitten	通信
8 月 24 日	疑似新 APT 组织针对土耳其海军发起钓鱼攻击		金融、教育
8 月 22 日	新 APT 组织 MURENSHARK 分析报告	MURENSHARK	军工、教育
8 月 22 日	TA558 组织对酒店、旅游行业的攻击活动追踪	TA558	旅游
8 月 19 日	黑客组织 APT41 对不同国家多行业组织发起恶意攻击	APT41	政府
8 月 18	APT 组织 Lazarus 通过发布虚假招聘信息传播恶意软件	Lazarus	互联网
8 月 18 日	俄罗斯黑客组织 SEABORGIUM 近期钓鱼活动披露	Gamaredon	政府、军工、教育、非政府组织
8 月 17 日	APT-C-35 全新升级，更新 Windows 攻击框架	APT-C-35	政府、军工
8 月 16 日	Gamaredon 黑客组织持续针对乌克兰发起攻击	Gamaredon	
8 月 15 日	APT27 组织利用聊天应用程序 Mimi 针对 Windows、Mac 和 Linux 用户	APT27	社交
8 月 12 日	Conti Group 利用 Exchange 漏洞攻击多个制造业相关公司	Conti	制造
8 月 12 日	UNC2447 通过窃取思科员工的凭证开展攻击活动	UNC2447	软件和信息技术
8 月 12 日	DeathStalker 利用 VileRAT 攻击世界各地的外汇和加密货币交易公司	DeathStalke	金融
8 月 11 日	deBridge Finance 加密平台被 Lazarus 黑客组织攻击	Lazarus	区块链
8 月 10 日	朝鲜黑客组织 Andariel 利用 Maui 勒索软件攻击医疗保健部门	Andariel	医疗
8 月 10 日	黑客组织 TAC-040 利用 Ljl 后门窃取信息	TAC-040	
8 月 9 日	TA428 利用新的 Windows 恶意软件部署后门进行间谍活动	TA428	工业制造、政府
8 月 9 日	APT 组织 Bitter 和 APT36 分发新型 Android 恶意软件	Bitter、Transparent Tribe	
8 月 8 日	APT32 组织利用 RemyRAT 木马攻击我国关键基础设施单位	APT32	政府

时间	APT 事件	组织名称	攻击行业
8 月 4 日	Kimsuky 通过 word 文档发送钓鱼链接	Kimsuky	
8 月 1 日	APT 组织 Gamaredon 对乌克兰政府发起多种网络攻击	Gamaredon	军工
7 月 26 日	疑似 APT39 组织利用 Konni 攻击欧洲多国	APT39	
7 月 25 日	黑客组织 TA4563 利用 Evilnum 恶意软件攻击欧洲金融和投资实体	TA4563	金融
7 月 22 日	挖矿团队 8220 Gang 将云僵尸网络扩展到三万台主机	8220 Gang	
7 月 21 日	APT29 利用合法通信服务 Slack 对意大利进行钓鱼攻击	APT29	政府
7 月 20 日	APT29 利用 DropBox 和 Google Drive 服务攻击多国大使馆	APT29	政府
7 月 19 日	朝鲜黑客组织 DEV-0530 利用 H0lyGh0st 勒索软件攻击中小型企业	Lazarus	非政府组织
7 月 18 日	Sidewinder 组织对巴基斯坦军事重点目标进行网络攻击	Sidewinder	通信、能源、航空航天、政府、军工
7 月 18 日	APT 组织蔓灵花再次针对孟加拉国开展攻击活动	BITTER	军工
7 月 15 日	UAC-0056 组织利用 Cobalt Strikes 再次以乌克兰为目标	UAC-0056	政府
7 月 15 日	APT 组织 Transparent Tribe 利用 CrimsonRAT 攻击印度教育机构	Transparent Tribe	教育
7 月 14 日	APT 组织 Confucius 利用木马后门攻击巴基斯坦政府机构	Confucius	军工、政府
7 月 13 日	CuteBoi 团伙利用 NPM 包进行大规模挖矿活动	CuteBoi	软件和信息技术
7 月 12 日	ITG23 组织针对乌克兰的攻击活动	ITG23	群众组织、政府
7 月 11 日	黑客组织滥用红队渗透工具 BRc4 进行攻击活动	APT29	
7 月 8 日	多个黑客组织使用 Royal Road 攻击俄罗斯实体	Space Pirates、Scarab APT、Mustang Panda、Tonto Team	
7 月 8 日	VSingle 恶意软件从 GitHub 获取 C2 服务器信息	Lazarus	
7 月 7 日	APT 组织 Bitter 继续瞄准孟加拉国	Bitter	军工
7 月 7 日	疑似 APT-C-23 组织伪装成通讯软件传播商业化木马	APT-C-23	军工、能源、教育
7 月 5 日	疑似 Confucius 组织攻击活动分析	Confucius	军工、政府、航空航天、外交机构
7 月 4 日	IIS 后门软件 SessionManager 已被 GELSEMIUM 威胁组织利用	GELSEMIUM	政府、非政府组织、军工
7 月 1 日	FoxAcid 渗透平台，带有后渗透能力	FoxAcid	
7 月 1 日	Confucius APT 组织近期活动分析	Confucius	宗教组织
7 月 1 日	攻击组织 Lazarus 使用恶意软件 YamaBot 针对双平台	Lazarus	软件和信息技术

天际友盟
TianJi Partners

专业的情报应用解决方案提供商

400-081-0700 www.tj-un.com
市场合作：mkt@tj-un.com 客户服务：service@tj-un.com 合作伙伴：partner@tj-un.com