CAICT 中国信通院 ThreatBook 微步在线

2020 年网络安全威胁信息研究报告

（2021 年）

中国信息通信研究院安全研究所
北京微步在线科技有限公司

2021 年 12 月

版权声明

本报告版权属于中国信息通信研究院和北京微步在线科技有限公司，并受法律保护。转载、摘编或利用其它方式使用本报告文字或者观点的，应注明“来源：中国信息通信研究院和北京微步在线科技有限公司”。违反上述声明者，编者将追究其相关法律责任。

前　言

2021 年 3 月 12 日，《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》正式发布，明确提出将“加强网络安全基础设施建设，强化跨领域网络安全信息共享和工作协同，提升网络安全威胁发现、监测预警、应急指挥、攻击溯源能力”作为发展规划之一，对国家网络空间安全提出了更高的发展要求。网络安全威胁信息作为发现网络威胁、抵御网络攻击的重要依托，助力信息安全防御手段向主动化、自动化、精准化转型，对于维护国家网络空间安全、建设数字中国具有重要意义。

2020 年新冠肺炎疫情爆发后，线上办公的广泛普及加剧了信息传递对网络的依赖，催生了愈加频繁的网络攻击行为。网络攻击的产业化发展趋势使得攻击工具和手法变得愈加复杂多样，传统的防火墙、入侵检测技术、恶意代码扫描、网络监控等被动防御手段显得捉襟见肘疲于应付。面对日益严峻的网络空间安全威胁，研究网络安全威胁信息有助于企业更好“知己”“知彼”，了解自身的网络安全脆弱点，掌握已知、未知的网络安全风险点，不断提升自身在实战中的检测与响应能力，筑牢网络安全防御城墙。

本报告从定义内涵、应用价值、标准化进展、政策和产业支撑等多个方面阐述了网络安全威胁信息的概念和发展现状。结合 2020 年全球网络安全威胁信息，从网络环境安全现状、常见网络攻击手法、受攻击行业和地域分布、国内较严重网络威胁及攻击事件等多维度系统性分析了 2020 年国内外网络安全形势。阶段性梳理了网络

安全威胁信息在国内重点行业的典型应用案例。最后，围绕发展中存在的标准化落地不足、共享机制缺失、产业成熟度较低等诸多问题进行了探索性思考，结合产业现状提出了针对性的意见和建议。对于本报告中的局限与不足，恳请各方同仁批评指正。

目 录

图 目 录

表 目 录

一、网络安全威胁信息概念及现状

本章详细阐述了网络安全威胁信息的定义内涵、层级模型和应用价值，并从国内政策导向、产业支撑情况和标准化进展等方面对网络安全威胁信息的发展现状展开说明。

(一) 网络安全威胁信息的概念

近年来，威胁信息逐渐成为网络安全行业的关注焦点，受到业界广泛讨论，如今已成为守护网络安全的重要手段。本节将从网络安全威胁信息的概念、意义和研发过程着手，对其技术理念、网络安全防护优势和研发工作特征展开介绍。

1.网络安全威胁信息的定义与内涵

综合国内外相关研究，我们归纳分析了多方定义后认为，网络安全威胁信息的核心内涵如下:

第一，网络安全威胁信息来源于对既往网络安全威胁的研究、归纳、总结，并作用于已知网络威胁或即将出现的未知网络威胁;

第二，网络安全威胁信息的价值是为受相关网络威胁影响的企业或对象提供可机读或人读的战术战略数据并辅助其决策，因此网络安全威胁信息需要包含背景、机制、指标等能够辅助决策的各项内容。

网络安全威胁信息的研究对象是“威胁”，包含已知的和即将出现的未知网络威胁，其内容既包括单一的木马样本、远控域名、攻击 IP 等基础数据，也包括安全事件、攻击团伙等概括性数据。“信息”是研究的结果，通过研究网络威胁的背景、机制、指标等内容，生产

出能够作用于该威胁的战术或战略数据，这些战术或战略数据就是“信息”。根据从简单到复杂的逻辑，“信息”可分为单一失陷指标、资产特征、时间画像、团伙画像、攻击者身份等不同的层次。简而言之，网络安全威胁信息是为研究网络威胁而提取出的，用于发现威胁、认识威胁、追踪威胁的数据。

2.威胁信息的网络安全防护优势

随着网络攻击技术的更新迭代，政府部门、企事业单位、社会组织等机构面临的网络威胁和挑战也愈加严峻。从传统的僵木蠕到勒索与虚拟币挖矿（Bitcoin Mining），从传统的漏洞利用套件（Exploit Kit）到供应链攻击，从传统的反检测到无文件攻击，攻击者的工具和手法愈发复杂多变、角度刁钻、难以检测。现有的杀毒软件、防火墙、网站应用级入侵防御系统（Web Application Firewall，WAF）等传统防护手段多为被动防御，仅根据已有策略在攻击发生时拦截攻击、阻止攻击生效并进行后续的恢复工作，对于策略之外的攻击则缺乏有力的检测和抵御手段。如何有效检测未知的网络威胁成为网络安全行业各方的共同着眼点。

网络安全威胁信息利用公开的可用资源预测潜在的网络威胁，通过对历史网络威胁的收集和处理提前预知攻击，在攻击发生之前就做好防御策略，帮助企业在网络安全防御方面更为积极主动，实现较为

精准的动态防御。根据 PPDR 安全防护模型[1]理论，威胁信息的网络安全防护优势主要体现在如下几个方面。

（1）检测方面：网络安全威胁信息能辅助用户对相关资产、风险、攻击面进行排查，从而让用户快速了解网络当前受攻击情况。

（2）防御方面：采取主动防御措施，对网络威胁进行精准打击。威胁信息提供的恶意 IP 地址、域名/网站、恶意软件 hash 值等失陷指标（Indicators of Compromise，IOC）能够直接用于网络安全系统和设备进行防护。

（3）响应方面：网络安全威胁信息能够帮助提供更完善的安全事件响应方案。

（4）预测方面：构建安全预警机制，不断收集有关新型网络威胁的信息数据，根据当前网络环境的薄弱环节有效预测可能的威胁，以帮助企业更好地应对未知威胁。

网络安全威胁信息的使用将有效提升报警准确性，降低无效报警数量，极大减轻安全运营人员工作压力，使其聚焦于真实威胁，提升工作效率，对政府部门、企事业单位、社会组织等用户机构的网络安全建设和运营具有重要意义。

3.网络安全威胁信息研发工作特征

[1]Gartner 在 2017 年发布的《应用保护市场指南》（《Market Guide for Application Shielding》，ID: G00337009）中，提出了由 Predict（预测）、Prevent（防护）、Detect（检测）、Response（响应）四个阶段组成的新 PPDR 闭环安全防护模型，该模型在安全防护不同阶段引入网络威胁信息、大数据分析等新技术和服务，旨在构建一个能进行持续性威胁响应、智能化、协同化的安全防护体系。

从 Gartner 提出概念开始，网络安全威胁信息已经发展了 8 年有余，形成了威胁信息研发的专业产线，研发工作的高度专业化、高成本特征日趋明显。

高度专业化：网络安全威胁信息研发的高度专业化体现在研发对象多元、研发产线环节多、数据数量质量要求高和研发人员专业性要求强等方面。**首先**，网络安全威胁信息研发产线涵盖原始数据、基础网络数据和网络威胁数据的采集、提取、分析等数据全生命周期管理，研发对象多元、研发环节多。**其次**，研发网络安全威胁信息依托于总量大、质量高的原始数据，即互联网公开的基础网络数据历史信息。原始数据经过处理后成为可用于威胁信息研发的基础数据，并由威胁信息研发工程师对其进行分析生成网络安全威胁信息。**再次**，网络安全威胁信息研发对研发工程师有较高的专业技术能力要求，研发工程师首先需要感知到新型网络威胁的存在，研究威胁的投递路径、关联关系等特点，搭建对应的网络安全威胁狩猎模型进行追踪，最终依赖不同类型的分析系统进行威胁分析和威胁信息的提取研发。

高成本研发: 网络安全威胁信息研发工作的高成本体现在**人力成本高、计算资源成本高**这两方面。随着跨国家、跨地区的全球化攻击日益猖獗，网络安全防护措施正逐渐由合规驱动转变为需求驱动，这就要求威胁信息需更为及时、准确。在数据收集阶段，需要积累时间跨度长、范围广的网络基础数据，并依托大量人力资源和计算资源投入对数据进行清洗、筛选，生成规模化的高质量数据。在网络安全威胁信息预测的模型训练阶段，依托于已有的规模化高质量数据，需要

经验丰富的威胁信息研发工程师对模型进行人工调优，进一步拉高了人力成本。

(二) 网络安全威胁信息能力层级模型

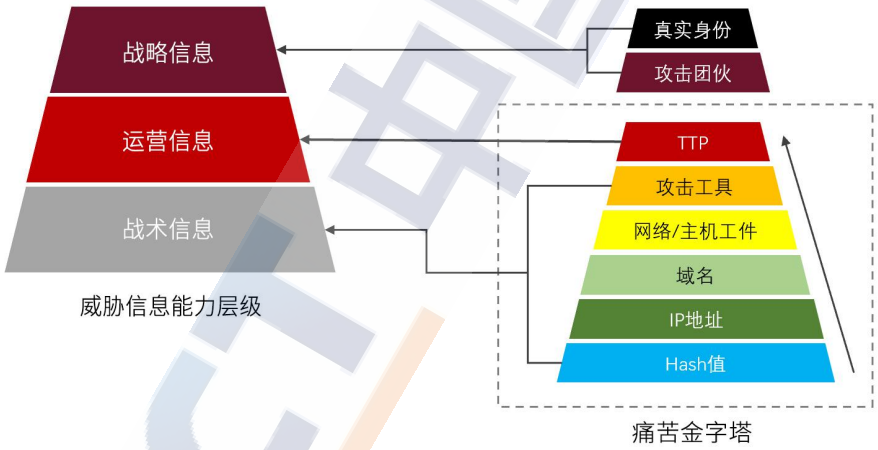
在研发和使用威胁信息时，不同的威胁信息复杂度和价值不尽相同，为了使威胁信息的研发和使用流程更清晰明了，需要根据失陷指标价值、安全能力和使用目的对威胁信息进行分类，以便应用于不同的场景。本节将详细描述“痛苦金字塔”威胁信息指标模型，并在此基础上基于使用目的对威胁信息进行分类，归纳出威胁信息能力层级模型。

资深安全专家 David J.Bianco 于 2013 年提出了“痛苦金字塔（The Pyramid of Pain）”威胁信息指标模型，并获得业内广泛认可。威胁信息的意义在于对已掌握的失陷指标做出快速响应，攻击者无法继续利用该指标发起攻击并由此感到痛苦，攻击者痛苦程度越高，该指标的价值也越高。“痛苦金字塔”模型根据攻击者的痛苦程度，将失陷指标价值划分了不同层级，由下至上分别为 Hash 值、IP 地址、域名、网络/主机工件、攻击工具、TTPs（Tactics、Techniques and Procedures，战术、技术和行为模式），其价值依次递增。

痛苦金字塔模型提出至今已有 8 年，模型中价值最高的 TTPs 指标已无法完全满足当前的安全需求，同时威胁信息研发技术的发展进步也赋予安全人员更完善的技术能力，挖掘更具价值的威胁信息，探知攻击团伙画像及其在现实世界中的真实身份。

因此，基于技术能力和安全需求的发展演进水平，本报告相应纳入了更具价值的威胁信息指标，对痛苦金字塔模型进行了扩展，模型各层级由下至上分别为 Hash 值、IP 地址、域名、网络/主机工件、攻击工具、TTPs、攻击团伙、真实身份，其价值依次递增。

威胁信息指标价值越高，其安全能力也越高，痛苦金字塔上层指标具备远高于下层指标的安全能力，可据此将威胁信息划分为三个递进的能力层级，不同的能力层级对应着不同的使用目的。最底层是以自动化检测分析为目的的战术级信息，中间层是以安全响应分析为目的的运营级信息，最高层是以指导整体安全投资策略为目的的战略级信息。



来源：中国信息通信研究院

图 1 威胁信息能力层级模型

战术级信息：位于威胁信息能力层级模型的最底层，对应痛苦金字塔模型中 Hash 值、IP 地址、域名、网络/主机工件、攻击工具等 5 个层级，其目的主要是自动化完成威胁发现、报警确认、优先级排序

等安全检测分析工作。例如 C&C[2]和 IP，二者都是可机读信息，可被设备直接使用并自动化完成上述安全工作。

运营级信息：位于威胁信息能力层级模型的中间层，对应痛苦金字塔模型“TTPs”层级，其使用者主要是安全分析师或安全事件响应人员，目的是分析已知的重要安全事件，如分析攻击影响范围、攻击链及攻击目的、技战术方法等，或者利用已知的攻击者技战术手法主动查找攻击相关线索。

战略级信息：位于威胁信息能力层级模型的最高层，对应痛苦金字塔模型的“攻击团伙”和“真实身份”层级，使用者主要是用户机构的安全管理者，如首席安全官（Chief Security Officer，CSO）等，其目的是帮助用户机构把握当前安全态势，更加有理有据地制定安全决策。战略级信息包含多方面内容，如预判和评估攻击者身份、攻击潜在危害、攻击者战术能力和资源掌控情况、具体攻击实例等。

在威胁信息能力层级模型中，自下向上每个层级的分析成果都作为其上方一层级的信息输入，层级越高，威胁信息研发难度越高、数量越少；相应地，攻击者攻击成本也随之增加，威胁信息对于被攻击者的价值也越高。

(三) 网络安全威胁信息的应用价值

网络安全威胁信息目前主要应用于企业网络安全防护、公共安全防护、国家安全防护等领域，相应的应用价值主要体现在提升企业主

[2]C&C：即 Command and Control 信息，攻击者控制被害主机所使用的远程命令与控制服务器信息。

动防御能力、助力打击网络犯罪行为、保护国家网络空间安全三个方面。

1.提升企业主动防御能力

随着广泛的企业“上云”趋势，云计算技术在生产办公环境中的大规模应用使得企业受攻击面变广，面临更加严峻的网络安全挑战。很多企业的安全防护以传统的防火墙、入侵检测技术、恶意代码扫描、网络监控等手段为主，在受到攻击后才采取措施，因此经常陷入被动防御的境地。

网络安全威胁信息能够提升企业对网络威胁的感知能力，让企业的安全防护由被动转向主动。威胁信息提供了多种网络安全防护操作，如攻击检测与防御、事件检测与响应、攻击团伙追踪、威胁狩猎、基于网络威胁发现驱动的漏洞管理、暗网信息发现等，能够有效降低网络威胁的平均检测时间与平均响应时间。在检测与响应阶段，威胁信息能够帮助企业快速识别攻击，明确攻击类型、意图和来源，利用上下文数据追溯攻击团伙，总结攻击者画像。在防护与预测阶段，威胁信息能够帮助企业在攻击发生前发现威胁，提前修复关键漏洞，变被动为主动，实现防御体系的关键性转变，提升企业安全防护能力，减少企业因网络威胁而遭受的损失。此外，行业内网络安全威胁信息共享能够汇聚具有相似特征的攻击事件，为精准溯源攻击者提供数据基础，提升行业内网络安全的联合防护水平。

2.助力打击网络犯罪行为

互联网技术飞速发展并广泛融入人们的生产生活，各种形式的网络犯罪也随之频繁发生，以黑产、灰产和暗网犯罪为主。黑产多利用网络开展违法犯罪活动，直接触犯国家法律，如电信诈骗、钓鱼网站、木马病毒、黑客勒索等；灰产多由正当行业衍生，游走于法律灰色地带，以恶意注册和虚假认证等方式为黑产活动提供便利，如为黑产运营社交账号、提供网络水军服务等；暗网犯罪是通过隐秘、特殊的登录方式与支付方式在难以追溯特征的网络空间从事犯罪活动。网络犯罪危害网络空间的公共秩序，严重侵犯社会组织和公民个人权益，打击遏制网络犯罪、追踪溯源犯罪分子是维护网络空间公共安全的重要议题。

通过分析处理恶意 IP 地址、域名网站、恶意软件 Hash 值、网络或主机特征、TTPs 等数据产出的威胁信息，能够完整还原犯罪团伙的组织名称、活跃时间、服务器和其他基础设备情况、攻击方向以及整体事件的来龙去脉，实现对网络犯罪的调查分析和记录留存，网络犯罪的线索共享、事件防范和预警，能够辅助案件侦破，抓捕犯罪嫌疑人，有效打击网络犯罪、改善网络环境，助力维护网络空间的公共安全。

3.保护国家网络空间安全

攻击者对国家政府部门、关键信息基础设施、关键行业机密的攻击越来越猖獗，网络空间如今已成为国家安全的又一重要角力场。金融、能源、电力、通信、交通等行业的关键信息基础设施一旦遭到攻击，可能导致交通中断、金融紊乱、电力瘫痪等严重后果，对国家安

全具有极大的破坏力与杀伤力；核电、军工、高校等领域的研发核心数据如果被窃取，可能会造成国家机密泄露，后患无穷。网络安全威胁信息能够检测与阻止内外威胁，增加黑客入侵成本，降低入侵速度，提升主动防御能力，确保组织提前做好准备，应对攻击，避免机密和数据泄露及资产损失，保护国家关键信息基础设施稳定安全运行。因此，各个国家的安全部门会持续跟踪全球活跃攻击者、生成威胁信息，并据此指导相关行业的网络安全防护工作，从而保障各行业关键基础设施安全性、核心数据安全性和核心业务连续性，从而保护国家安全。

(四) 网络安全威胁信息领域发展现状

1.国内相关政策文件要求

网络安全威胁信息的研发和应用已成为一项安全防护必备技能，受到安全厂商、用户机构和监管部门的广泛认可，国家及相关主管部门陆续出台了一系列与网络安全威胁信息相关的政策、标准等文件，如《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》《信息安全技术 网络安全等级保护测评要求》（以下简称等保 2.0）、《关键信息基础设施安全保护条例》（以下简称《关基条例》）等。针对工业互联网、虚拟现实、5G、数据中心等细分领域的网络威胁信息工作，工业和信息化部（下称“工信部”）陆续出台多项政策进行了规划和部署，发布了《加强工业互联网安全工作的指导意见》（工信部联网安〔2019〕168 号）、《5G 应用“扬帆”行动计划（2021-2023 年）》（工信部联通信〔2021〕77 号）等

指导性文件，将构建网络安全威胁信息能力视为维护国家网络空间安全和各领域网络安全的一项重要手段。

此外，工信部已连续多年组织开展网络安全试点示范工作，并将网络安全威胁监测与处置作为重点引导方向之一，以增强企业防范和应对网络安全威胁的能力。网络安全试点示范工作延续至今，威胁监测已成为 5G 网络、车联网、物联网、人工智能等多个新型信息基础设施安全的重点工作内容之一，威胁信息作为网络安全公共服务的核心环节备受重视。

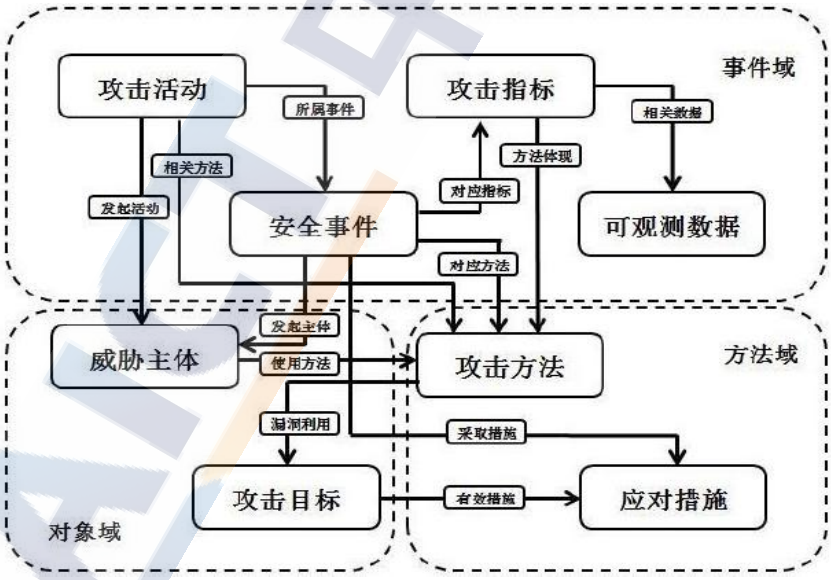
2.国内标准化工作进展

制定网络安全威胁信息标准具有重大意义。通过规范化威胁信息的格式，业内对网络安全威胁信息的描述就可以达到一致，使用户间、系统间的上传下达等流转工作更加高效顺畅，提升威胁信息的共享效率和行业整体的网络威胁态势感知能力。

在网络安全威胁信息共享方面，美国较为领先，已提出一些威胁信息共享交换标准。目前国外已经有多种较为成熟的网络安全威胁信息格式，并得到不同程度的应用。《美国联邦信息系统安全和隐私控制建议》（《Security and Privacy Controls for Information Systems and Organizations》NIST 800-53）、《美国联邦网络威胁信息共享指南》（《Guide to Cyber Threat Information Sharing》NIST 800-150）、结构化威胁表达式（Structured Threat Information eXpression，STIX）、网络可观察表达式（Cyber Observable Expression，CyboX）以及指标信息的可信自动化交换（Trusted Automated eXchange of Indicator

Information，TAXII）等都为国际网络安全威胁信息的交流和分享提供了可靠参考。威胁信息的标准制定和优化能够有力推动其技术发展和共享进程，然而，到目前为止，暂时没有一个能够在国际上通用的相关标准。

2018 年 10 月 10 日，我国正式发布国内首个网络威胁信息的国家标准——《信息安全技术 网络安全威胁信息格式规范》（GB/T 36643-2018），并于 2019 年 5 月 1 日正式实施。该标准从可观测数据、攻击指标、安全事件、攻击活动、威胁主体、攻击目标、攻击方法、应对措施等八个组件进行描述，并将这些组件划分为对象、方法和事件三个域，最终构建出一个完整的网络安全威胁信息表达模型。该通用模型能够统一业内对网络安全威胁信息的描述，进而提升威胁信息共享效率和网络威胁态势感知能力。



来源：《信息安全技术 网络安全威胁信息格式规范》

图 2 网络安全威胁信息表达模型示意图

规范网络安全威胁信息的格式和交换方式是实现网络安全威胁信息共享和利用的基础与前提，在推动网络安全威胁信息技术发展和产业化应用方面具有重要意义。该标准适用于供需双方之间的网络安全威胁信息生成、共享和使用，为网络安全威胁信息共享平台的建设和运营提供参考，指导产品间、系统间、组织间的威胁信息共享和交换，提升整体安全检测和防护能力，在多个层面支撑国家网络安全工作。在国家级态势感知能力构建层面，标准提供了不同层级系统间统一的威胁信息上传下达格式，有助于快速建立态势感知机制；在行业级通告预警信息共享层面，标准提供了统一的预警信息格式，条件允许的场景下，能形成可机读的检测和防护规则，有助于大幅缩短响应时间；在产业级安全防护协同联动层面，标准有助于不同厂商产品间的自动化交互，提升产业整体能力水平。然而，我国现行的网络安全威胁信息国家标准距离在业内广泛落地实行仍有一定差距，标准在描述字段、适应业务能力和接口标准上仍有较大提升空间。

3.国内网络安全产业支撑

（1）建立健全威胁信息共享联动机制

工信部牵头组织建设了工业和信息化部网络安全威胁和漏洞信息共享平台[3]（简称 NVDB 平台），督促网络产品提供者合理发布自身产品安全漏洞，鼓励漏洞收集平台和其他漏洞发现组织和个人主动

[3] 工业和信息化部官网：《工业和信息化部网络安全威胁和漏洞信息共享平台正式上线运行》（https://www.miit.gov.cn/xwdt/gxdt/sjdt/art/2021/art_930f57bc7b584d188f07303d4c48b730.html）

报送漏洞信息，支持开展网络安全产品漏洞技术评估，督促网络产品提供者及时修补产品安全漏洞。

（2）行业自律共建网络威胁信息联盟

2016 年 2 月，国家互联网应急中心与中国互联网协会网络信息安全工作委员会联合发起成立了中国互联网网络安全威胁治理联盟（CCTGA），宣布建立专业领域协作机制，联合网络安全领域上下游力量，加强全国网络安全纵深防御体系建设，有效整治互联网地下黑色产业相关威胁，为净化网络环境和维护网民利益的起到了积极作用。

2019 年 3 月，上海市信息安全行业协会协同连尚网络、平安科技、顺丰集团等发起成立“威胁数据共享联盟”。该联盟重点共享治理网络威胁的知识体系和信息，通过平台化模式累积网络威胁最佳解决路径，威胁数据脱敏后变成一种可供他人获取的知识模式，进行策略分配到执行的知识库，供联盟内企业进行比对查询，共同推进威胁数据领域的新技术新应用，维护行业安全稳定发展，提升数据治理与安全防御能力，打造安全创新生态圈。

网络安全威胁信息产业联盟聚集了安全产业上下游企业，为其提供了资讯互通和资源整合的新渠道，成员间的监督协作有助于加强我国网络安全行业自律和社会治理水平，为打破威胁信息孤岛、保障新时期网络安全提供了强劲动力。

二、2020 年国内外网络安全威胁信息分析

本章将基于 2020 年网络安全威胁信息，从网络威胁变化趋势、攻击手法、国内外易受攻击行业和地域等维度对 2020 年网络安全态势进行研究分析，并盘点 2020 年国内较严重的网络威胁类型。

(一) 2020 年国内外网络威胁情况概览

2020 年国内外网络安全态势较以往更为严峻。据 Check Point[4]和 SonicWALL[5]观测，在 PC 端一直都有活跃表现的勒索软件在 2020 年全年呈激增态势，并造成严重危害。勒索软件开始利用基于暗网的云基础设施进行数据的分批次泄露，以此威胁被勒索组织，迫使其尽快交付赎金；随着世界范围内移动设备感染率的上升，IoT 设备被感染的可能性也大大增加；黑客对供应链、VPN、漏洞等常见攻击面的兴趣仍然在持续，并且开始出现伪装成 Zoom、Slack 等通讯工具客户端进行攻击的现象；此外，黑客及黑产组织仍然在暗网上持续活动，并被监测到存在利用暗网买卖泄露数据、云基础设施等行为；在 2020 年，被曝光的 APT 攻击事件有数百起，40 余个国家和地区遭受了不同程度的 APT 攻击。

2020 年的新冠肺炎疫情对网络环境也产生了一定影响，尤其在网络攻击方面，与新冠肺炎疫情相关的攻击数量大幅度上升，攻击手段更加多样，医疗行业受此影响较大，移动办公相关的信息基础设施和远程通讯工具是受攻击重灾区，新冠肺炎疫情及冠状病毒相关的话题成为攻击者偏好的诱饵。

[4]数据来源于《全球威胁指数》报告，由头部网络安全解决方案提供商 Check Point 软件技术公司的网络安全威胁信息部门 Check Point Research（CPR）于 2021 年 5 月发布。

[5]数据来源于《2020 年威胁报告》（《2020 SonicWall Cyber Threat Report》），由头部互联网安全设备及平台提供商 SonicWALL 于 2021 年发布。

2020 年网络威胁的变化趋势主要体现在以下几个方面。

（1）移动端和固网端感染率大幅上升

Nokia 的观测数据[6]表明，受新冠肺炎疫情影响，在 2020 年 2 月和 3 月，移动端感染率比前几个月增加了近 30%，在 5 月和 6 月，固定宽带网络的感染率也出现大幅度上升，但 Nokia 并未披露具体数据。

（2）冠状病毒相关域名数量大幅增加

Akamai 的数据[7]显示，2020 年 1 月 1 日到 2020 年 4 月 1 日，超过 90,000 个以冠状病毒为主题的域名被注册，尽管其中很大一部分域名与恶意行为无关，但攻击者的确注册了大量与新冠肺炎相关联的欺诈性域名。此外，由于疫情期间医疗机构的业务量增加，信息化系统需要录入更多患者数据，面临更大运营压力；为了保证业务连续性，医疗机构在受到勒索攻击后交付赎金的意愿更高，因此可能会更容易受到勒索攻击。

（3）疫情相关垃圾邮件大规模出现

趋势科技的数据[8]显示，2020 年全年至少有超过 1600 万个与新冠肺炎疫情相关的网络威胁被检出，包括恶意 URL、垃圾邮件和恶意软件，这些网络威胁大部分来自美国、德国和法国。在各类网络

[6]Nokia 于 2020 年发布的《Threat Intelligence Report 2020》

[7]业界头部内容交付网络（CDN）服务提供商 Akamai 于 2020 年发布的《[state of the internet]/security: A Year in Review》

[8]全球头部安全整体解决方案提供商趋势科技（Trend Micro）于 2021 年 2 月发布的《A Constant State of Flux: Trend Micro 2020 Annual Cybersecurity Report》

威胁中，垃圾邮件占比近 90%，攻击者将其作为首选攻击渠道，相较于恶意 URL 和恶意软件，垃圾邮件有着更低的技术门槛。

（4）针对远程办公场景的攻击手段增加

疫情期间，当员工居家办公时，攻击者也正在利用电话会议软件发起更多攻击行为，模仿电话会议提供商的应用程序以分发恶意软件，例如创建与 Zoom、Microsoft Teams、Google Hangouts 等远程办公软件类似的恶意域名等。

（5）攻击者活跃度显著提升，攻击指向性愈发明显

攻击者的主要攻击对象是从事疫苗开发、生物医疗研究、政策制定的机构和组织，攻击者会调整钓鱼诱饵，冒充疫情相关信息引诱攻击对象操作，从而窃取其核心数据。攻击者通过钓鱼网站和垃圾邮件等方式诱导攻击对象打开钓鱼附件，传播 Emotet、Trickbot、远控、后门、DDoS 和挖矿等木马，并以此进行攻击。

(二) 2020 年国内外网络攻击手法概览

根据现有数据统计，2020 年全球失陷主机约有 6,431,498 台，国内约有 880,607 台，约为全球的 1/8 左右。

从全球范围来看，攻击者的主要攻击对象未产生较大变化，邮件、云服务、VPN、移动设备、IOT 设备仍然是受害重灾区；攻击手段上，钓鱼、勒索软件、供应链攻击、利用漏洞、社会工程学等仍是攻击者的主流选择。

从国内受攻击情况来看，大多数攻击来自于国内攻击者，而威胁集中表现为设备被利用于挖矿，这也反映出目前国内黑客黑产等攻击

者的主要目的是获得经济利益。国外已经出现勒索和窃取数据融合的攻击手法，产生的危害较大，建议国内相关机构持续重视这一趋势。此外，利用木马远程控制主机进行 DDoS 攻击、下载恶意软件等行为也在持续发生，蠕虫等病毒传播引发的计算资源、带宽资源的消耗仍然值得重视。

下面将详细盘点 2020 年全球网络攻击的主要手法和发展趋势，并简要探讨应对措施。

1.钓鱼邮件仍是主流攻击手段

2020 年，攻击者仍旧广泛使用电子邮件展开攻击活动，传播各种网络威胁。欧盟网络安全局（ENISA）[9]指出，“攻击包括诸如基于企业工程的电子邮件攻击（BEC）和身份欺骗技术等计划，以使网络钓鱼活动更有效”，“超过 99％的分发恶意软件的电子邮件需要人为干预（包括点击链接、打开文档、接受安全警告和其他行为）才能有效”。

钓鱼邮件的发件者会模仿成信誉良好的组织或机构，其目标通常是窃取身份验证数据等敏感信息、安装恶意软件或获取信用卡号等其他财务资源。一部分钓鱼攻击属于鱼叉式网络钓鱼，具有高度针对性，但是无确定攻击对象的“广撒网”式钓鱼攻击活动更为普遍。钓鱼邮件诱使收件人点击指向恶意站点或文件的链接、或打开附件（通常是压缩文件或 Microsoft Office 文件），在某些钓鱼邮件中，接收者还必须启用编辑或宏才能触发感染。

[9]ENISA Threat Landscape

但是，网络钓鱼技术也在不断发展。趋势科技在 2020 年观察到[10]，攻击者开始使用在线表单（例如生成在线调查问卷的工具）来托管网络钓鱼站点。相比假冒域名和网站，创建表单的时间成本和技术门槛更低，表单创建者仅借助表单生成器就能制作简单的页面，虽然与精心构建的伪造域名相比较为简陋，但这也意味着即使是没有经验、技术水平较低的网络犯罪分子也可以毫不费力地开始网络钓鱼攻击。

未来较长一段时间内，网络钓鱼攻击将变得越来越常见，并可能和勒索软件、APT 攻击等手段相结合，诱饵和所用邮箱也将和企业机构信息有更高的相关度。安全人员可适当开展网络安全培训、网络钓鱼模拟演练等工作，定期督促员工警惕钓鱼攻击的风险和危害，提升员工网络安全意识，防止被网络钓鱼。

2.远程办公普及，VPN 攻击带来网络安全新挑战

新冠肺炎疫情防控的要求催生了远程办公的兴起，但是边界、隔离模糊和大量远程终端的接入也给办公网络带来了新的安全挑战。根据趋势科技的观测[10]，VPN 作为常见的应对手段，2020 年的使用率达到了历史最高水平。

VPN 已经成为新的攻击面和风险来源。根据 Zscaler 的数据[10]，CVE 数据库中已经列出了将近 500 个 VPN 漏洞；在企业当中，93％的用户正在使用 VPN 服务，同时，94％的用户知道网络犯罪分子将 VPN 定位为目标，以获取对网络资源的访问权限；72％的用户担心

[10]云安全公司 Zscaler 于 2021 年发布的《2021 VPN Risk Report》

VPN 可能会损害 IT 部门保持其环境安全的能力；67％的用户正在考虑替代传统 VPN 的远程访问；目前，72％的用户将优先考虑采用零信任模式。

随着疫情防控常态化，远程办公网络的 VPN 攻击也将成为中大型用户必须面对的挑战之一。对于多分支机构、多办公地点、员工地域流动较大的企业和组织，安全人员须找到一种既精准有效、又易于部署和统一管控的网络防护方案，如利用 DNS 解析技术对撞威胁信息等，否则将存在攻击者从分支机构或员工远程终端攻入总部办公网络的风险。

3.勒索软件产业化特征明显，攻击手法出现新变化

为了追求经济利益，攻击者对于攻击对象的选择更具针对性，不同于以往的随机选择方式，现阶段勒索软件攻击对象更关注具有高价值资产的关键行业；且攻击手法更加多样，包括利用未修补的漏洞、滥用弱的远程桌面协议（RDP）安全性、采用其他恶意软件家族等。

Ryuk 和 Sodinokibi 是目前最知名的勒索软件，它们在很大程度上定义了现代勒索软件格局。2020 年还出现了一些相对较新的勒索软件，例如 Egregor 和 DoppelPaymer，两者都已有成功实施勒索的案例[11]。勒索软件运营商还一直在将其目标范围扩展到更多操作系统，例如，RansomExx 并非 2020 年最常被检测到的勒索软件，但它对 Linux 服务器的攻击能力却不容小觑，其主要目标是 VMware 环境，即用于存储 VMware 文件的计算机。

[11]A Constant State of Flux：Trend Micro 2020 Annual Cybersecurity Report.

此外，勒索手法也出现了新的变化，过去受害者只需要担心其数据被加密或删除，而现在的攻击者将定位高价值数据，不仅会删除或加密受害者的数据以进行勒索，还会通过泄漏站点（DLS）间接泄漏被盗数据，这种手法可被理解为 Big Game Hunter（BGH）的演进[12]。2020 年，BGH 的态势趋向于迫使受害者一旦被勒索软件感染就马上进行勒索谈判。2020 年 10 月，SunCrypt 勒索软件的运营商使用 DDoS 攻击迫使受害者支付赎金，这是 BGH 攻击者在 2020 年“广为人知”的新攻击策略。受害者往往迫于被加密数据和文件的重要性而交付赎金，令攻击者总能达到攻击目的，增长其嚣张气焰，使得近几年勒索赎金呈指数级增长。根据保险公司 Coalition 的数据[13]，仅在 2020 年上半年，Coalition 保单持有人中，被勒索软件攻击的频率就增加了 260%，平均赎金需求增加了 47%，金额达 338,669 美元。

根据 CrowdStrike 观测到的数据[13]，2020 年受勒索软件泄露数据影响最严重的排名前四的行业分别是工业和工程领域（229 起）、制造业（228 起）、科技行业（140 余起）、零售业（140 余起）。值得注意的是，制造业尤其容易受到勒索软件的攻击，如果由于系统故障而无法满足生产需求，那么该企业不仅要承担因勒索软件感染造成的数据泄露、支付高额赎金等损失，日常运营的中断还会极大地影响核心业务。

对于被勒索者来说，若被加密的数据或文件事前没有备份，除了交赎金购买密钥以外，就只有重做终端或服务器的系统，而勒索后的

[12]CrowdStrike 于 2021 年发布的《2021 Global Threat Report》
[13]Bennett Jones LLP：2021 Ransomware Insurance Update, Explosion of Ransomware and Best Practices

数据泄露则是攻击者的又一个勒索筹码。要做好勒索软件的防护，最可靠的方式是构建全面的网络威胁检测响应体系，引入能快速更新的网络威胁信息库，勒索事件一旦在其他国家、地区、行业领域发生，网络威胁信息库便发挥协助检出相关勒索事件和勒索团伙的功能。此外，应当做好关键核心数据文件的备份工作，防止勒索软件删除、加密数据造成的数据永久性丢失。

4.供应链攻击成为规避网络安全防御措施的新攻击手段

攻击者通常很难直接攻击政府部门、大型金融机构等拥有强大网络安全系统的用户机构，但可能将供应链作为一种间接攻击途径。由于用户机构的网络安全设备只能对自身网络资产进行盘点，而对供应链攻击的筛查则需要用户机构和供应商的多方配合。对供应链攻击缺乏警惕的用户机构会默认供应商的产品和服务可以安全交互并开展业务，攻击者利用用户机构及其供应商之间的信任模型，通过损害供应链中安全性较低的部分，规避网络安全系统的防御措施侵入目标系统，间接达成攻击目的。

在全球范围内的供应链攻击已十分严重。SolarWinds 公司被攻击是 2020 年最受关注的供应链攻击事件之一。SolarWinds 公司是美国基础网络管理软件供应商，拥有大批美国政府部门客户。2020 年 3 月至 6 月期间，攻击者将 SolarWinds 公司的商业软件更新程序木马化，以污染供应链的方式入侵了北美、欧洲等地区的政府、科技、电信等重要领域的组织和机构，最终实现了窃取信息的目的。事件披露后更多受害者浮出水面，美国国防部、商务部、财政部、国土安全部

等政府机构，火眼、微软等科技公司均受到波及。供应链攻击通常极难防御检测，此次攻击活动从开始实施到被披露至少经过半年的时间，攻击者拥有充足的机会对核心目标单位进行进一步攻击，影响范围远超近年的 Xcode、CCleaner、Xshell、phpStudy、驱动人生等软件供应链攻击事件，媒体报道称“美国正遭遇史上最严重黑客袭击”。

国内目前已开始供应链防护的初期探索，金融、互联网等行业已开始探索自动化的供应商风险评估体系，并取得一定成效。供应商风险评估的主要步骤为：事前充分了解供应商信息；事中持续监控、自动化评估；事后量化评估结果并自动改进。该体系能够对供应商的风险、资产图谱和安全控制能力进行持续综合评估，并展现各供应商的安全动态评分和趋势走向。未来这一风险评估方法论或将在国内广泛落地。

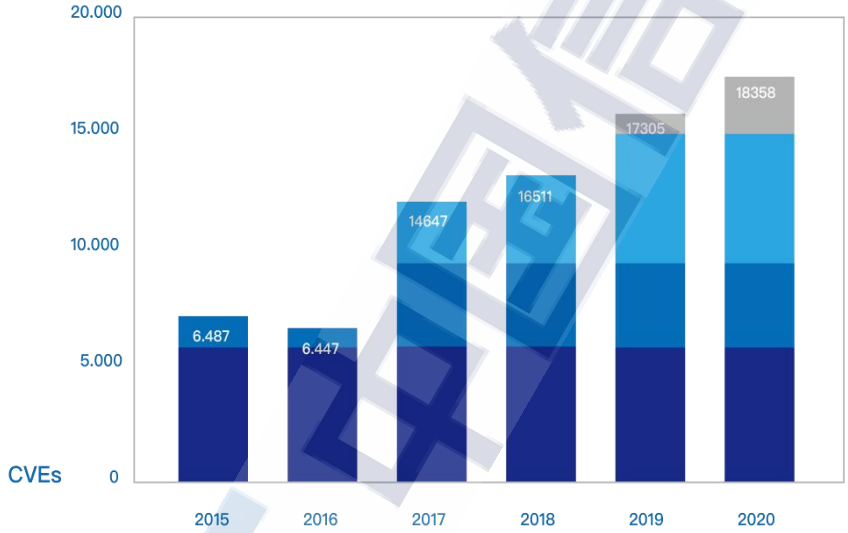
5.漏洞威胁严重，老漏洞持续被利用，新漏洞大量被披露

漏洞仍是当前网络安全的重大威胁之一。攻击者主要使用未修补的漏洞，并将多个漏洞链接在一起，从而发起一次完整的攻击。根据 Skybox Security[14]和 Tenable[15]的数据，2015 年到 2020 年间通用漏洞（CVE）数量增长态势明显，平均年增长率 36.6%；2020 年全球范围内 CVE 报告数为 18358 个，相比 2019 年的 17305 个，增加了 6%，相比 2015 年的 6487 个，涨幅高达 183%；从 2020 年 1 月到 10 月，

[14]数据来源于网络安全管理及安全分析服务商 SkyBox Security 于 2020 年发布的半年度报告《2020 Vulnerability and Threat Trends》

[15]数据来源于网络安全软件厂商 Tenable 的安全反应小组（SRT）于 2021 年 1 月发布的《2020 年威胁形势回顾》（《2020 Threat Landscape Retrospective》）

全球有 730 起公开披露的外泄事件，共导致超过 220 亿份记录泄露；Google Chrome、Mozilla Firefox、Internet Explorer 和 Microsoft Edge 等网页浏览器一直是零日漏洞的主要目标，占所有被野外利用的零日漏洞的 35%以上。目前可追溯到的是，2005 年的漏洞仍在被大量利用，用户不应认为自己的系统可以免受因旧漏洞而造成的侵害，应始终保持警惕，及时下载安装相应的软件补丁，同时，用户也应持续关注新增的漏洞，尤其是零日漏洞。



来源：Tenable

图 3 近年已通报的 CVE 漏洞数量

国内方面，从国家互联网应急中心到各大互联网厂商的安全应急响应中心（SRC），各机构对漏洞的重视从未减轻，对于漏洞的防护和管理工作也已经取得一定成果。安全人员应定期进行漏洞排查，定时检查终端、服务器是否已经打好补丁，同时要积极关注网络安全事件，出现突发网络事件时快速启动应急响应措施，进行应急处理和追踪溯源。

6.隔离网渗透的危害逐渐被认知

理想情况下，物理隔离可以有效阻断传统的基于网络路由可达的网络攻击，确保隔离内网生产环境的安全稳定。然而，隔离网络系统注定要牺牲网络数据交换的便捷性，为了解决实际生产环境中的数据交换需求，操作人员可能会被迫做出一些风险性极高的操作，譬如搭建内网跳板机映射共享目录、使用可移动存储设备进行数据摆渡等，这些操作相当于间接打通一条与外网通信的隧道，破坏了物理隔离的完整性。

2020 年 5 月，DarkHotel 组织一款名为 Ramsay 的攻击工具被曝光，该工具可在物理隔离网络中收集信息，且无网络行为，属于定制性木马。Ramsay 可通过被感染的软件安装包进行传播，该程序在隔离网络的主机上被运行后，会执行.exe 文件进行感染、内网扫描、文档收集等行为，将收集到数据加密压缩并附加在正常文档中，待这些文档被带出隔离网络并接入其他被控设备后，攻击者就能够成功提取窃取的数据，实现对隔离网络的攻击。Ramsay 是继 Stuxnet（震网）攻击事件、Flame 蠕虫、CIA 网络武器库 Vault7、NSA 秘密武器 COTTON-MOUTH 等隔离网突破组件后的又一典型事件。

隔离网渗透攻击行为的危害在全球范围内逐渐被认知，但国内对此认知仍不够充分。安全人员应当注意对隔离网络主机和 DMZ 区域的防护，做好网络间的流量监控，引入威胁信息等手段持续进行监测工作。

7.攻击者仍旧活跃，攻击手法多样

2020 年新冠肺炎疫情期间，攻击者仍旧活跃。根据观测发现，中国、美国、韩国、印度、巴基斯坦、乌克兰等国家和中东、欧洲等地区是 APT 攻击最大的受害者，政府、军事、外交、科技、金融、医疗、能源、教育等行业和领域是攻击者的主要目标，攻击发起者主要来自于南亚、东南亚、朝鲜半岛和中东地区。此外，攻击对象不再单一聚焦于 Windows 平台，跨平台的 APT 攻击已成为主流。成熟度较高的攻击者如海莲花、Lazarus、Turla、APT28 等均实施过跨平台的攻击活动，攻击主要集中于 windows、Linux 和 Android 平台，少量出现在 MacOS 和 IOS 平台。

表 1 攻击者攻击活动平台分布

攻击者\OS 平台	Windows	Linux	Android	MacOS
孔夫子（Confucius）	有		有	
蔓灵花（Bitter）	有		有	
响尾蛇（SideWinder）	有		有	
肚脑虫（Donut）	有		有	
海莲花（Oceanlotus/APT32）	有		有	有
Lazarus	有	有	有	有
危险密码	有			
DarkHotel	有			
Kimsuky	有		有	
Konni	有		有	
绿斑	有			
Gamaredon	有			
APT28	有	有		
Turla	有	有		
WellMess	有	有		
APT35	有			
MuddyWater	有			
APT-C-23	有		有	
StrongPity	有			

来源：网络安全威胁信息服务商

在攻击者的攻击手法方面，挖矿伪装是较为引人注意的新趋势。一直以来，挖矿是攻击者攻陷主机后的主要活动之一，然而根据最新研究，攻击者开始将自身的攻击伪装成挖矿行为，从而掩盖自己的真实行动（如安装后门、窃取数据等），安全人员需要对此加以重视。2020 年，攻击者通过定向钓鱼邮件诱导攻击对象执行恶意文档植入白利用木马，然后以该主机为据点对目标企业内部进行横向渗透，通过在失陷主机部署门罗币挖矿木马程序，以此隐藏其高级攻击的行为，即使攻击对象发现网络中的异常，也会判定为挖矿活动选择忽视或低优先级处理，从而忽略了攻击者的真实目的。

在攻击的组织形式方面，攻击发起者的佣兵化趋势日益明显。具有国家背景的攻击者多以窃取科研数据、危害他国安全等为目的发起攻击。同时，现已出现针对商业公司的以收集商业机密为目的的攻击者，为潜藏暗处的雇主服务。2020 年 8 月，国外安全厂商曝光了一个在全球范围内开展攻击活动的黑客组织 DeathStalker，该组织的攻击对象主要是金融科技公司、律师事务所和财务咨询机构，他们并不实施安装勒索软件、窃取支付信息等常见黑产活动，而是专注收集商业机密。该安全厂商因此判断 DeathStalker 具有雇佣兵性质，攻击活动主要是为其雇主服务，此类黑客团伙并非具备国家背景的攻击者，但对大多数商业公司产生的威胁更大。

相比其他网络威胁，APT 攻击的侵入更隐秘，会使用内核级木马、无文件攻击等手法避开常规的检测响应工具，有些 APT 攻击事件中，攻击者甚至会擦除自己的移动痕迹。这就要求安全人员了解攻击者近

期活动，掌握攻击者常用的攻击手法、攻击工具和 IP、域名等相关失陷指标（IOC），从攻击全链条对 APT 攻击进行发现和处置。

(三) 2020 年国内外网络受攻击情况分析

1.国内外网络攻击受害行业分析

放眼国际，IBM X-Force 的数据显示[16]，金融和保险业已连续第五年成为受攻击最多的行业，制造业从 2019 年的第八位跃居 2020 年第二位，而能源行业从 2019 年的第九位跃升到 2020 年的第三位，这可能是攻击者开始关注对基础设施、工业控制设备的入侵所致。

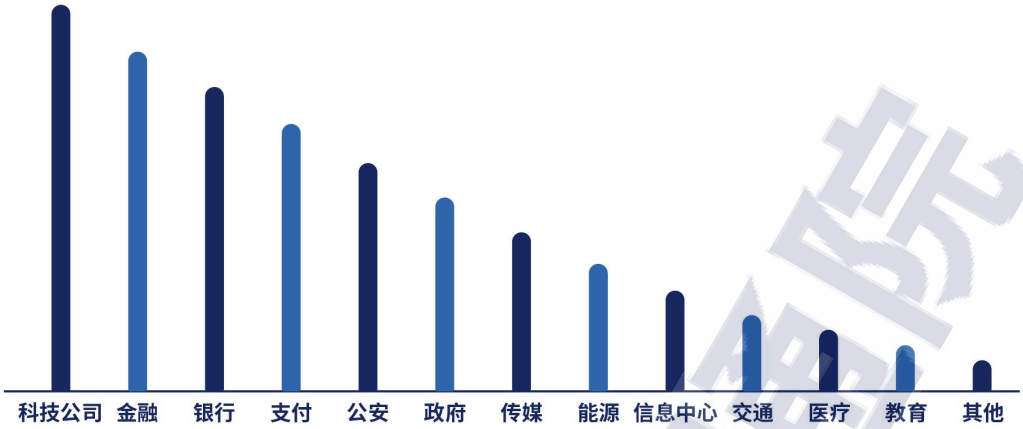
表 2 国外网络攻击受害行业分析与对比

行业	2020 年排名	2019 年排名	排名变动
金融和保险	1	1	-
制造业	2	8	**↑ 6**
能源	3	9	**↑ 6**
零售	4	2	↓ 2
高端服务业	5	5	-
政府	6	6	-
医疗健康	7	10	**↑ 3**
媒体	8	4	↓ 4
交通	9	3	↓ 6
教育	10	7	↓ 3

来源：IBM X-Force

着眼国内，在 2020 年，大金融行业仍然是黑客黑产组织攻击欲望最高的对象，金融、银行、支付三项总和在观察到的受攻击网络环境总数中占比 38.2%，此外，政府与公安受攻击占比 17.7%，科技类公司受攻击占比 16.7%，能源、信息中心、交通、医疗、教育等行业也受到不同程度的网络攻击。

[16]IBM Security 于 2021 年发表的《X-Force Threat Intelligence Index 2021》



来源：中国信息通信研究院整理

图 4 国内各行业受攻击情况占比

从行业属性来看，金融、能源、科技、医疗等是全球范围内受攻击较多的行业，国外的制造业、零售业和高端服务业（如酒店等）受攻击情况也较为严重。相比之下，国内这三个行业尚未受到较多攻击，但随着我国 IT 信息化水平的提高，各行业上云工作持续推进，制造业、零售业、高端服务业等目前尚处于攻击低频状态的行业将面临更加严峻的网络安全环境。此外，政府、传媒、信息中心、交通、教育等行业和领域的网络攻击情况也值得关注。

2.国内外网络攻击受害地域分析

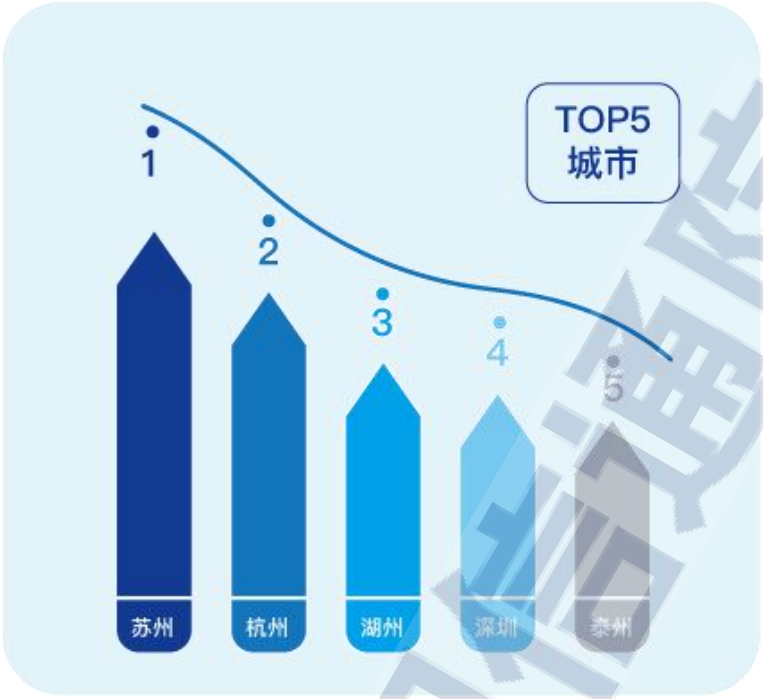
从国际地域层面来看，根据 IBM Security 数据[18]，2020 年，欧洲、北美和亚洲承受了全球大部分攻击，这一情况与往年一致，但这几个地区受攻击占比有所变化。2020 年有 31％的攻击发生在欧洲地区，27%的攻击发生在北美地区，25%的攻击发生在亚太地区。其中，欧洲地区的受攻击占比大大高于 2019 年的 21％，跃升为 2020 年全球受攻击最多的地区；而北美地区的受攻击占比较 2019 年的 44%有下

降明显，这一趋势可能是欧洲和亚太地区受攻击增加所致；亚太地区虽然受攻击占比相较 2019 年的 22％高了 3 个百分点，但 BEC 攻击事件少于其他地区，这可能是由于亚洲用户倾向于实施多重身份验证，使得仅凭钓鱼邮件成功攻击的几率下降。

从国内地域层面来看，2020 年失陷主机最多的五个省份分别为江苏、浙江、安徽、广东和台湾，分别为 149,899 台、123,690 台、82,756 台、81,614 台和 44,440 台，失陷主机最多的五个城市分别是苏州、杭州、湖州、深圳和泰州。

来源：中国信息通信研究院整理

图 5 2020 年国内失陷主机最多省份



来源：中国信息通信研究院整理

图 6 2020 年国内失陷主机最多城市

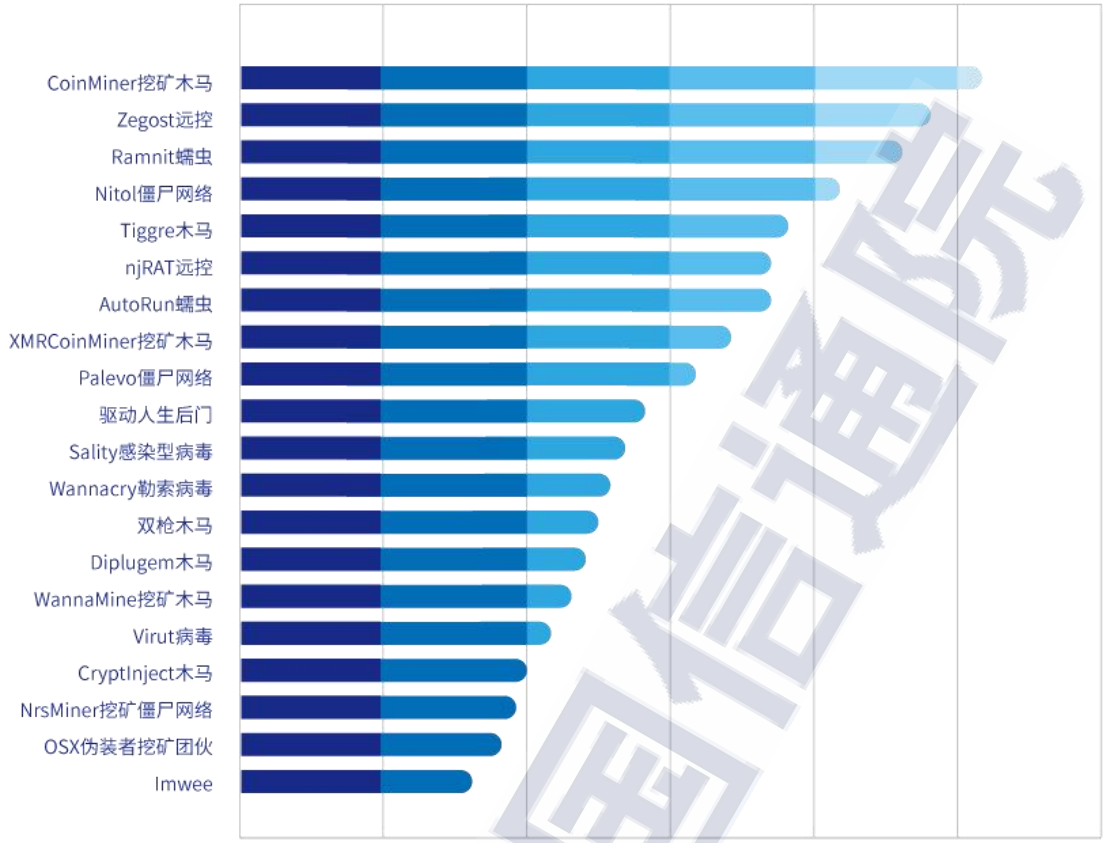
国内失陷主机分布最多的长三角、珠三角辐射地区，是我国经济相对发达的区域，也是整体信息化水平较高的区域。然而失陷主机最多的 5 个城市中无一为省会城市，且仅深圳一座一线城市，北京、上海和广州并未上榜，这可能与一线城市和省会城市的网络安全防护措施相对完善有关。

综上所述，在江苏、浙江、安徽、广东等经济发展较快、网络安全水平未及时跟上的行政区块中，应当继续贯彻落实等保 2.0、《关基条例》等制度，因地制宜进行网络安全相关政策法规的推动落实，把先进的网络安全技术、产品、解决方案和服务下沉覆盖，除了每年定期的攻防演练外，还需定期清查主机失陷情况，排除网络环境中的已有威胁。

(四) 2020 年国内较严重网络威胁盘点

2020 年 1 月开始，新冠肺炎疫情引起政府高度关切和民众广泛讨论，大量不同背景的黑客组织闻风而动，伺机对我国网络空间展开攻击。攻击者以新冠病毒相关的高社会关注度话题为诱饵，通过钓鱼网站和垃圾邮件传播 Emotet、Trickbot、远控、后门、DDoS 和挖矿等木马软件，攻击者冒充疾病预防控制中心、病毒学家和公共卫生中心等，通过警告所在地区出现新的感染案例、声称提供安全措施、提供感染列表等话术诱导收件人打开钓鱼附件进行攻击。

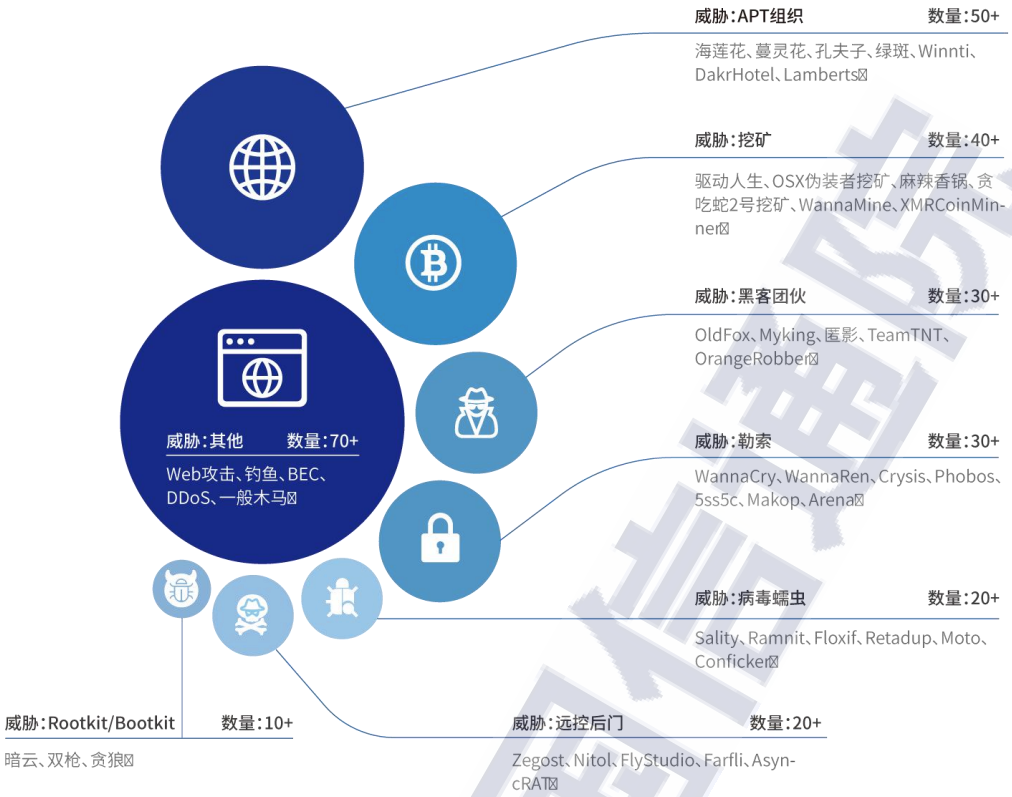
在 2020 年国内各类高级网络威胁中，从综合危害程度的维度，僵尸网络、木马、蠕虫、远控/后门等仍然是影响较大的高级威胁，挖矿、勒索、数据窃取、资源消耗、远程控制是其造成的主要危害。在抽样调查中，排行前三位的 Nitol 僵尸网络、CoinMiner 挖矿木马和 XMRCoinMiner 挖矿木马感染了 1/3 的网络环境，Bladabindi 后门虽然感染的网络环境较少，却是目前监测环境中命中次数最多的高级威胁，总命中数达到 8.8 亿次。



来源：中国信息通信研究院整理

图 7 综合危害程度最强的 20 种高级威胁

从应急响应的维度分析，在 2020 年全部应急响应案例中，16.7%的应急响应需求来自攻击者的攻击，13.3%由挖矿导致，约 10%的威胁来源于国内的黑客/黑产团伙，勒索类应急响应占 10%，病毒蠕虫、远控后门、Rootkit/Bootkit 病毒、Web 攻击、钓鱼、BEC、DDoS 等威胁亦有发生。



来源：中国信息通信研究院整理

图 8 应急响应维度占比分析

三、网络安全威胁信息典型应用实践

威胁信息的本质是知识，如何在具体场景将知识落地并取得成效，是在各行业开展网络安全威胁信息应用的核心问题。立足我国具体国情和网络安全需求，目前国内威胁信息应用落地有以下几个方向可供参考。

一是结合检测技术。在安全产品研发阶段，将威胁信息与流量分析、终端检测技术相结合，落地为基于网络安全威胁信息的检测响应类产品，部署在用户机构对应的网络环境中。**二是建立共享机制**。对于分支部门较多的用户机构，建立本地威胁信息管理平台，构建网络威胁信息库和威胁信息共享机制，提高网络威胁挖掘研发和应用能

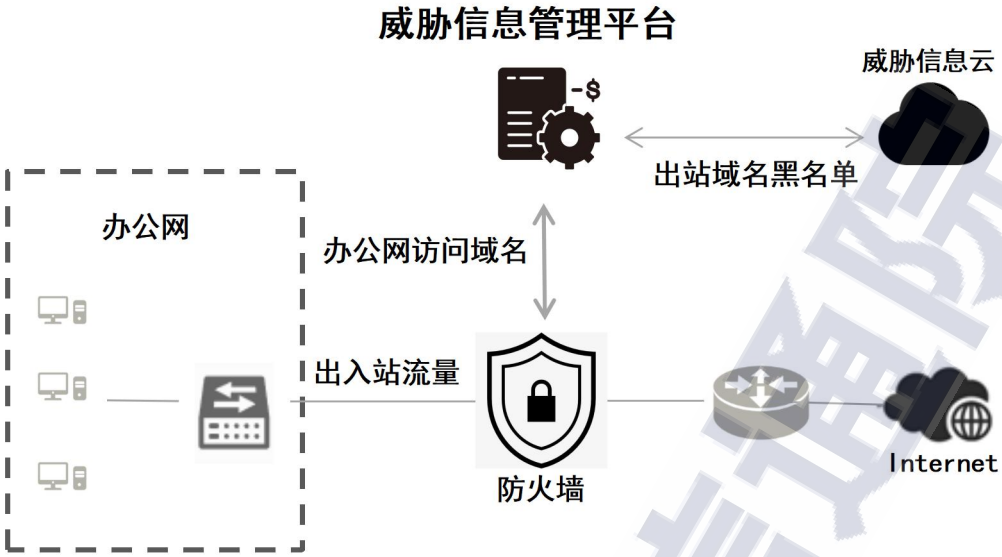
力。**三是联动安全设备**。联动其他网络安全设备，如 IDS/防火墙、日志大数据平台等，与现有处置知识库与工单系统构建闭环处置流程，提升用户机构网络安全的整体检测响应能力。

基于上述落地方向，本章将列举电子信息制造商、基础电信企业、网络视频平台和云计算服务商等工业和信息化行业中的典型场景应用案例，探讨网络安全威胁信息在信息化产业的落地实践。

(一) 电子信息制造商实践案例

近年来，电子信息制造业已成为我国国民经济的重要支柱产业，并逐渐呈现国际化趋势。电子信息制造商往往在全球有多个办公区域，员工多、终端多，网络架构复杂，开展网络安全防护工作有一定难度。存储了高价值知识产权与先进设计文件或数据的主机或服务器，容易成为黑客攻击目标，企业数据资产和知识产权的保护工作迫在眉睫。

在本案例中，企业办公网有一个统一的流量出口，流量出口处串联接入防火墙，对网络出站流量进行全面的监控，通过威胁信息管理平台与防火墙的闭环协作运营机制，从防火墙中剥离出内网访问请求的对应域名，以.syslog 的形式传送给威胁信息管理平台，威胁信息管理平台以其内置的高质量 IOC 进行碰撞分析，将确定的恶意域名回传给防火墙，防火墙将收到的恶意域名添加黑名单并自动进行拦截与告警。威胁信息管理平台定期与威胁信息云进行数据同步和更新，确保失陷威胁发现和威胁拦截的准确性和及时性。



来源：网络安全威胁信息服务商

图 9 电子信息制造商威胁信息管理部署

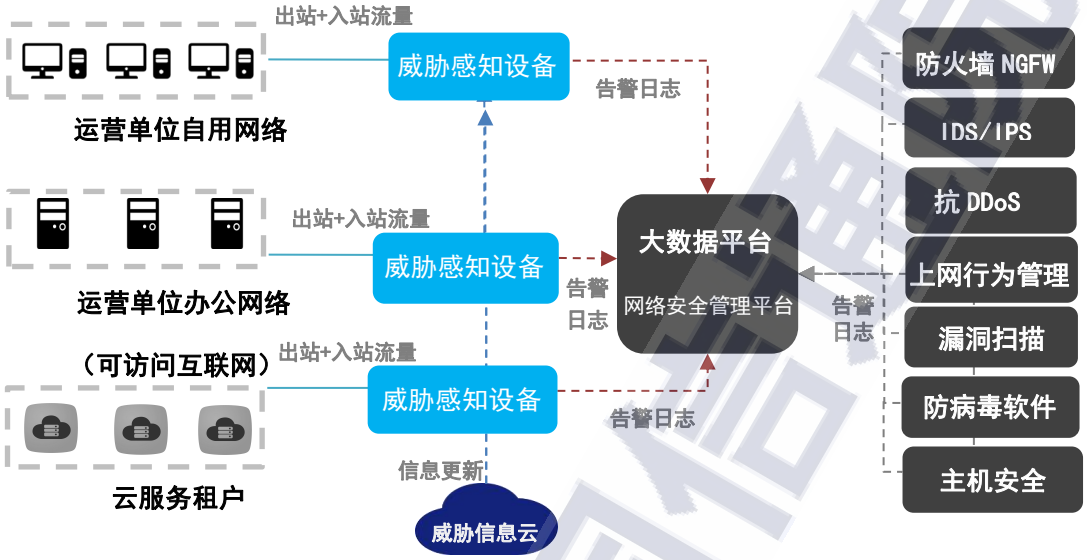
该电子信息制造商在企业网络内部部署威胁信息管理平台，并与防火墙对接，一方面，结合防火墙中网络出站访问日志，碰撞威胁信息管理平台中高质量 IOC 失陷指标（域名、IP），弥补防火墙的内网失陷威胁检测能力；另一方面，利用威胁信息管理平台的联动能力，实现防火墙对外连恶意通信的自动化阻断。

(二) 基础电信企业实践案例

基础电信企业承载了海量公民个人信息以及网络流量信息，由此成为攻击者窃取数据的重点攻击目标。

在本案例中，该基础电信企业选择利用威胁信息赋能的威胁感知设备对云租户网络、企业自用网络、企业办公网的出入站全流量进行检测，将告警日志统一接入大数据平台，实现企业网络威胁检测能力的全覆盖，提升高级威胁发现识别能力，并与现有处置预案知识库与

工单系统联动，形成高效的运营处置闭环，提升了对网络威胁的检测和响应能力，为业务的稳定连续增加了一道防线。



来源：网络安全威胁信息服务商

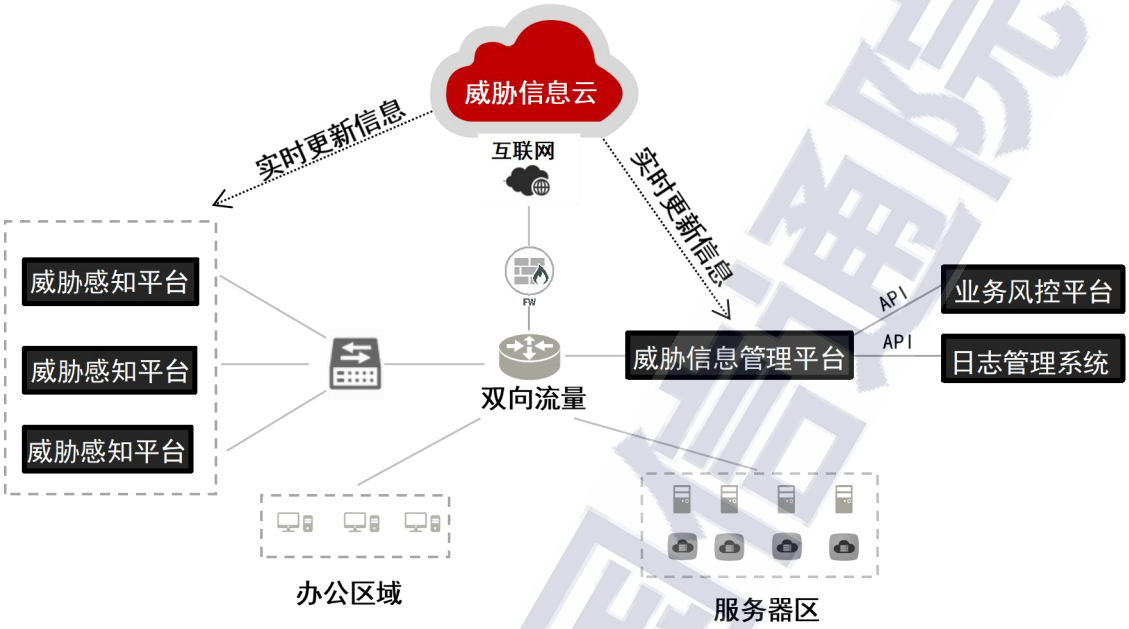
图 10 基础电信企业威胁信息管理部署

(三) 网络视频平台实践案例

随着新型攻击手段、未知威胁的出现，加之网络视频平台所处的互联网行业计算能力与大数据高度集中化，网络攻击呈现出更高的复杂性、隐蔽性、针对性趋势，被动防御模式很容易被绕过。内部业务创新需求不断升级，外部安全威胁不断加剧，双重因素影响给网络视频平台的安全能力建设提出了更高要求。

本案例中，该网络视频平台选择通过威胁信息赋能超大流量威胁感知设备。一方面，通过流量镜像实时检测可能的威胁，加强对未知威胁的发现和识别，并结合现有处置制度进行工单流转，形成高效的运营处置闭环。另一方面，实现威胁信息管理平台与 ELK 日志系统、业务风控系统对接联动，利用威胁信息过滤筛选 ELK 海量日志，并

且赋能业务风控形成多维度分析因子，提升平台异常风险用户识别精准度。



来源：网络安全威胁信息服务商

图 11 网络视频平台威胁信息管理部署

在本案例中，该网络视频平台基于应用场景设计部署威胁信息管理平台，填补了自身安全体系的攻击事件提取能力，提高了网络攻击检测响应效能，满足企业的网络安全需求。同时基于应用场景需求严格把控网络安全威胁信息准确度，避免出现大面积封禁造成用户无法访问平台的现象，也符合业务风控的安全要求。

(四) 云计算服务商实践案例

随着越来越多的政企业务向公有云、政务云迁移，云端已成为黑客、黑产团伙的又一攻击目标。作为云服务提供商，需要提升云端整体的安全检测与分析能力，在海量的攻击中识别真实威胁，并对暴露

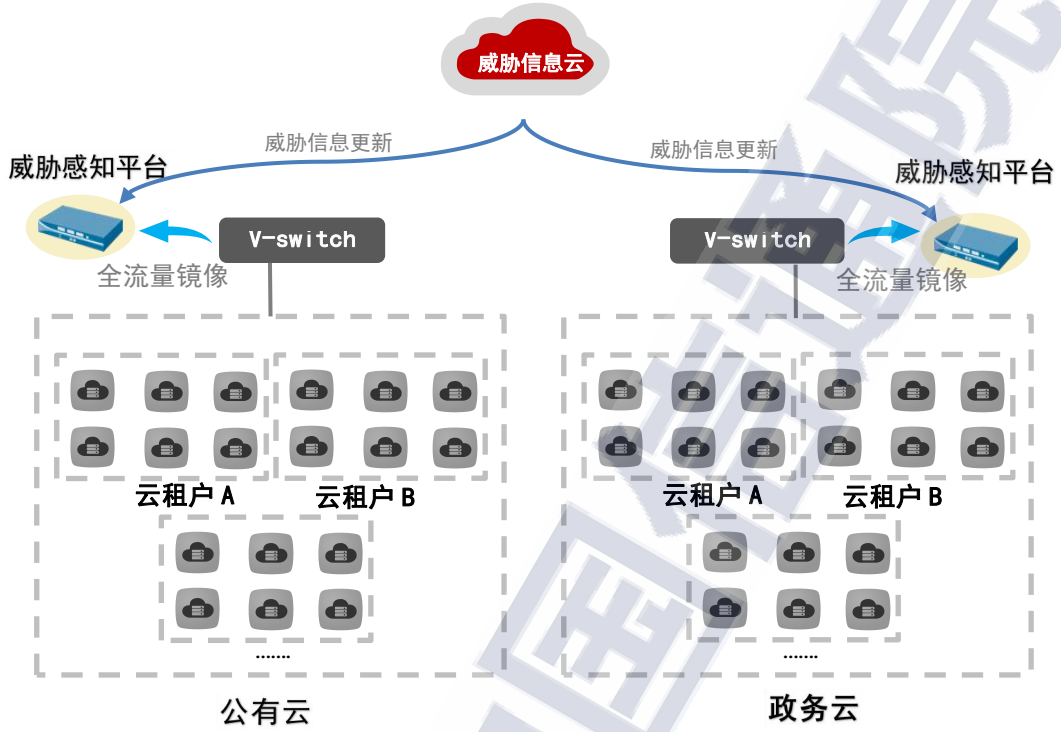
资产进行全面梳理，提升云服务提供商对租户的安全运营能力，帮助租户应对安全威胁，并满足合规要求。

在本案例中，云计算服务商为租户提供公有云和政务云服务，需要提升公有云安全运营团队内部失陷发现与响应能力，也需要提升政务云租户威胁感知与资产风险识别能力。因此，该云计算服务商选择了部署具备威胁信息能力的威胁感知设备，发现内部威胁、检测外部威胁、识别资产风险，针对公有云和政务云两个服务场景采取了不同的解决方案。

对于公有云，依托威胁信息进行失陷主机检测、定位以及取证分析，完成处置闭环。在公有云网络出口位置部署具备威胁信息能力的威胁感知设备，并旁路镜像接入出站方向流量及内部 DNS 日志；利用威胁信息发现内部失陷主机，并对失陷主机内网渗透路径、数据窃取等行为进行描绘。

对于政务云，依托威胁信息，覆盖各租户的外部攻击感知、内部失陷威胁、资产风险梳理需求。在政务云网络出口位置部署具备威胁信息能力的威胁感知设备，并旁路镜像接入出入站双向流量；利用威胁信息、行为规则、机器学习、沙箱等技术，对外部攻击、内部失陷、内网横移、加密、数据窃取等全攻击链威胁进行检测，并将敏感行为、告警结合威胁信息进行智能聚合完整还原攻击路线，并描绘黑客画像；利用旁路监听，对租户应用系统暴露的服务、域名、端口、IP，以及管理后台、弱密码、API 接口等资产风险进行全面梳理；通过安

全运营平台，对各租户的威胁事件和资产风险进行分离和独立呈现，为各租户提供安全增值服务。



来源：网络安全威胁信息服务商

图 12 云计算服务商威胁信息管理部署

四、网络安全威胁信息应用建议

(一) 推进标准体系建设 完善行业共享机制

目前，国外已有多个网络安全威胁信息报文格式在使用，但不同厂商间未形成通用标准。因国内标准化工作起步较晚、产业融合不足等原因导致我国国内现行的网络安全威胁信息标准距离在业内广泛落地应用尚有一定差距。网络安全威胁信息跨平台、跨系统、跨厂商流转存在较大阻碍，制约了威胁信息共享机制和安全防御体系的建立健全。

在标准体系建设方面，建议**一是**立足国外行业标准和国内行业实际需求，持续优化现行国家标准，推进国家标准验证点建设和反馈联动机制建立，制修订立足我国国情的网络安全威胁信息系列标准，不断提高标准通用性和有效性水平；**二是**加强标准研制与科技创新协同对接，开展产学研用广泛合作，凝聚业界广泛共识和力量，推动科技研发、标准研制与产业化协同发展；**三是**按照全国标准化工作部署开展机器可读标准探索和试点工作，细化、统一报文字段、系统接口等技术规范，为机器自动处理奠定规则基础，消除跨平台、跨系统、跨厂商对接协作技术壁垒，提升网络安全威胁信息的自动化处理能力和行业流转共享水平。

(二) 坚持效果评估导向 构建联动协同业态

我国威胁信息的发展仍存在产品性能和匹配度不足、共享机制缺失等诸多问题，网络安全威胁信息产品及服务提供商要充分利用自身深厚技术储备、丰富实践经验和产业牵引作用，以网络安全防护效果为能力评估导向，直面市场痛点，完善技术产品和服务水平，积极推进产业协同，探索产业发展路径。

一是强化研发创新能力。网络安全威胁信息产品及服务提供商要着力提升专业技术实力和产品研发能力，聚焦亟需补齐的技术短板开展核心技术攻关，增强优质产品供应能力。在满足《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规要求的前提下，以强化威胁信息产品防护效

果为出发点，不断优化、更新和迭代产品技术，提升准确性、时效性、可扩展性等多方面产品性能。

二是优化精准服务能力。提升市场对接水平，为用户提供定制化、专业化、贴身化服务，依托自身经验积累和技术积淀，以安全体系防护效果为导向，为威胁信息用户提供系统性的安全建设建议和合规指导，助力用户安全体系由被动防御向主动防护转变，释放威胁信息单点赋能效能。

三是深化产业牵引能力。头部网络安全威胁信息产品及服务提供商要充分发挥对产业高质量发展的核心引擎功能和辐射带动作用，探索和实践更切实可行的网络威胁认定和共享机制，为产业协同联动发展提供强有力支撑，发挥“头雁效应”带动建立威胁信息共享平台和联动体系，构建威胁信息协同共享的健康业态，提升威胁信息协同水平和安全防护能力。

(三) 强化主体责任意识 筑牢安全防御体系

《网络安全法》《数据安全法》《关基条例》等法律法规的陆续出台，进一步明确了网络安全对于国家安全的重要性，彰显了我国守护网络空间安全的决心。随着等保 2.0 对信息系统的网络安全威胁信息能力提出具体明确要求，威胁信息建设势在必行。政府部门、企事业单位、社会组织等机构作为威胁信息的最终用户，要强化安全主体责任意识，完善安全性自我评估制度，健全内部安全防御体系。

一是政策和市场双驱动。用户机构根据自身业务实际需求和面临的主要安全威胁，对照国家政策法规、标准等相关要求明确网络安全

建设目标、重点内容和保障措施，结合网络安全威胁信息的覆盖度、准确度、可用性、可扩展性和专业度等多方面因素综合评估产品性能，政策合规和市场需求双轮驱动，规划设计可落地的网络安全防御体系构建方案。

二是严格规范威胁信息选用标准。网络安全威胁信息源选择方面，坚持威胁信息数量与质量并重，保障信息丰富全面的同时，避免大量低置信度信息淹没严重安全事件；多源威胁信息选择方面，提升不同来源威胁信息的差异性，通过网络威胁信息管理系统整合多源威胁信息，优化威胁信息准确性和覆盖面。

三是融入安全体系加快落地部署。应加快推进威胁信息体系落地部署，充分利用已有安全能力，联动已有安全系统和设备，将事件响应、自动化编排与威胁信息系统进行结合，切实将威胁信息能力融入现有安全架构中，建设威胁信息检测系统、威胁信息库、威胁信息本地管理平台、威胁信息在线查询平台等系统，充分利用威胁信息改善安全运营工作，筑牢网络安全防御体系。

(四) 完善从业培训机制 提高人才培养水平

网络安全威胁信息研发产线复杂，涉及数据处理环节众多，对模型精准分析和训练有较高要求，严重依赖工程师的专业能力和技术经验。建议建立完善的从业人员培养培训机制。

一是提升安全素养。加强威胁信息知识宣传普及，积极推动将威胁信息纳入网络安全教育体系，广泛吸纳网络安全从业人员开展威胁信息研发及使用技术研究，做好从业人员持续培训，加强后备人才培

养力度，法律合规教育、技术能力提升、安全意识强化三管齐下，不断提高威胁信息人才安全素养，为产业发展输送高层次人才。

二是促进人才交流。广泛开展行业研讨，聚集核心岗位人员和关键人才分享技术进展和最佳实践方案，以人才交流促进威胁信息相关技术和经验在业内自由流动，提升威胁信息应用整体水平。

CAICT 中国信通院

中国信息通信研究院 安全研究所

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：010-62300264

传真：010-62300264

网址：www.caict.ac.cn