IBM Security

IBM X-Force 威胁情报指数 - 2020 年

IBM

IBM X-Force 事件响应和情报服务 (IRIS) 编制

目录

目录

摘要和关键趋势

IBM Security 开发了各种智能企业安全解决方案和服务，帮助您的企业增强抵御未来网络安全威胁的能力。

为了让安全专业人员了解最相关的威胁，IBM X-Force 会定期发布有关新兴威胁及攻击者所用战术、技术和程序 (TTP) 的博文、白皮书、网络研讨会和播客。

IBM Security 每年都会发布 IBM X-Force 威胁情报指数报告，其中会总结我们的各个研究团队在过去一年中发现的最突出威胁，向安全团队提供相关信息，以帮助他们更好地保护其组织。

本报告中提供的数据和洞察力来自 IBM Security 托管的安全服务、事件响应服务、渗透测试活动及漏洞管理服务。

IBM X-Force 研究团队分析了来自数亿个受保护端点和服务器的数据，以及来自非客户资产（如垃圾邮件传感器和蜜网）的数据。IBM Security 研究团队还在全球范围内运行垃圾邮件陷阱，每天监控数以千万计的垃圾邮件和钓鱼攻击，分析数十亿个网页和图像，从中检测攻击活动、欺诈活动和品牌滥用，以更好地保护我们的客户以及我们所处的互联世界。

X-Force 事件响应和情报服务 (IRIS) 汇编了 IBM Security 在过去一年的软件和安全服务分析结果，这些结果显示 2019 年是旧威胁以新方式再度粉墨登场的一年。

- X-Force 的分析数据显示，2019 年针对运营技术 (OT) 的攻击事件数量增长了 2000%，这可能预示着：随着我们迈入 2020 年，威胁实施者对攻击工业系统的兴趣“日渐浓厚”。

- 2019 年，共有超过 85 亿条记录遭到泄露，比 2018 年丢失的记录数量高出 200% 以上。疏忽的内部人员是造成这种剧增的主要原因。2019 年，86% 的记录由于服务器配置错误（包括可公开访问的云存储、不安全的云数据库以及未适当予以安全保护的同步备份或开放的互联网连接网络区域存储设备）而遭到泄露。

- 这种恶意软件威胁格局在 2019 年发生了变化，威胁实施者重新开始使用勒索软件并建立了僵尸网络。2019 年，X-Force IRIS 响应了 5 大洲 12 个国家或地区的勒索软件活动，这些活动涉及 13 个不同的行业。此外，破坏性恶意软件活动的情况表明，这种潜在的灾难性恶意软件趋势仍然是一个不断上升的威胁。

- 在 X-Force IRIS 于 2019 年进行的互动中，排名前三位的初始入侵媒介所占的比例非常接近，占比分别为：钓鱼攻击 (31%)、扫描与漏洞利用 (30%) 和凭证被盗 (29%)。最值得注意的是，钓鱼攻击在 2018 年占事件总数的近一半，而到 2019 年，其占比不足三分之一。相比之下，扫描与漏洞利用所占比例从 2018 年的 8% 增加到了 2019 年的近三分之一。

- X-Force 对全球垃圾邮件活动分析后得出结论，垃圾电子邮件会继续使用有限的漏洞，尤为值得关注的只有两个 CVE：2017-0199 和 2017-11882。这两个漏洞均为已修补的漏洞，在威胁实施者尝试通过垃圾邮件活动利用的漏洞中占比近 90%。

- 尽管金融服务在 2019 年依然是受攻击数量最多的行业，但从行业特定的攻击目标也可以看出威胁实施者的优先攻击目标有所变化，零售、媒体、教育和政府在全球最常受到攻击的行业排名中均有所上升。

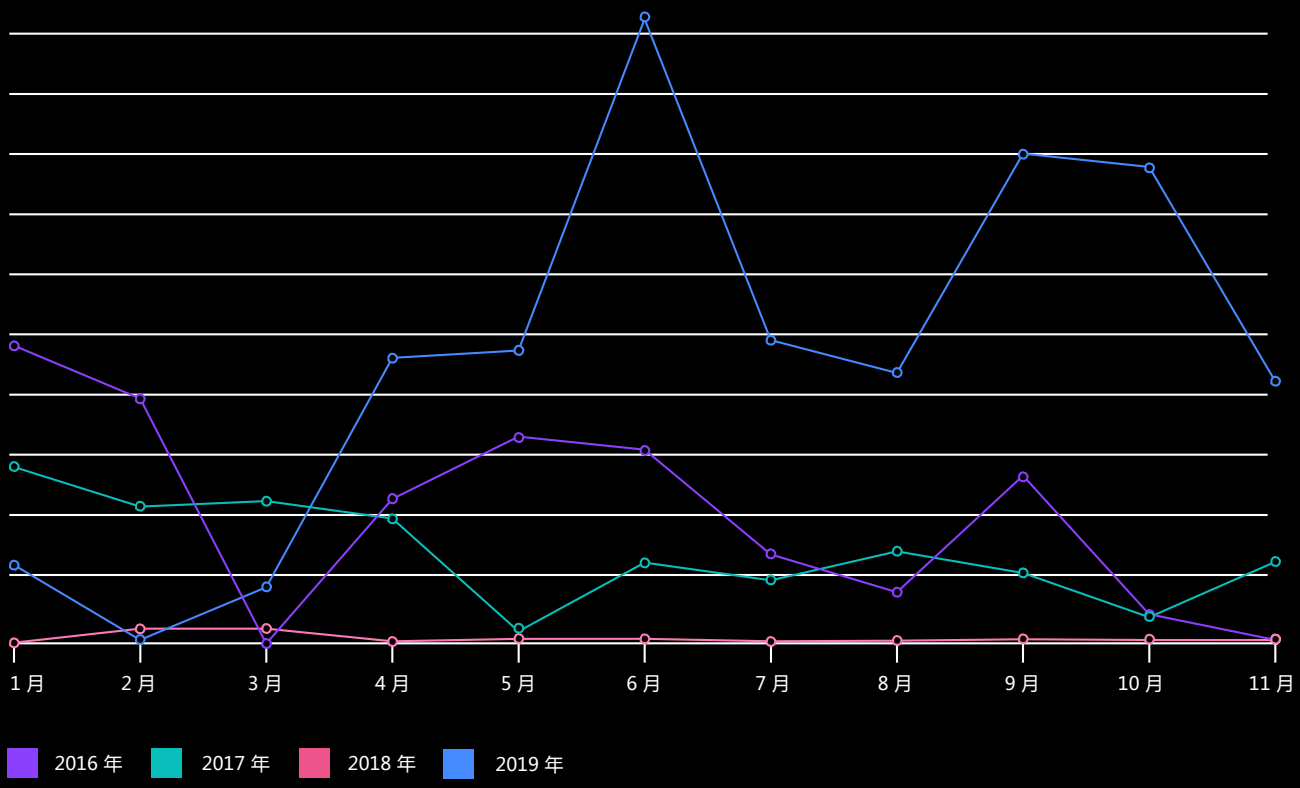
- 今年的 X-Force 威胁情报指数报告新增了全球中心洞察，旨在提供在全球范围内监测到的趋势数据。IBM Security 在今年继续跟踪了针对所有地区的多种威胁实施者，而本报告重点介绍了针对每个地区的主要威胁实施者、从 2019 年开始监测到的攻击以及在 2020 年可能需要重点关注网络安全的一些日期。

本年度报告的以下各节介绍了各方面的主要趋势，并深入研究了形成 2019 年威胁格局背后的因素。

目标及初始入侵媒介

图 1：
运营技术 (OT) 攻击趋势

月 OT 攻击量 - 对比 2016-2019 年的数据（来源：IBM X-Force）



针对运营技术 (OT) 基础架构的攻击呈爆炸性增长趋势

IBM X-Force 分析数据表明，自 2018 年以来，威胁实施者针对工业控制系统 (ICS) 及类似运营技术 (OT) 资产的攻击事件增加了 2000% 以上。实际上，2019 年针对 OT 资产的事件数量超过了过去三年监测到的活动数量总和。

大多数监测到的攻击都是使用 SCADA 和 ICS 硬件组件内已知漏洞组合实施的攻击，以及使用蛮力登录策略针对 ICS 目标进行的密码喷雾攻击。

据报道，一些针对 ICS 的攻击活动与两个已知的威胁实施者有关，而且与我们在遥测中监测到的攻击时间轴激增不谋而合。Xenotime 组织和 IBM Hive0016 (APT33) 发起了两次特定活动，据报道，他们都扩大了对 ICS 目标的攻击。

IT 基础架构和 OT 之间的重叠，例如可编程逻辑控制器 (PLC) 和 ICS，会继续给 2019 年依赖此类混合基础架构的组织带来风险。

IT/OT 基础架构的融合使得 IT 漏洞攻击者可以将目标锁定在控制物理资产的 OT 设备，这就可能会大幅增加恢复成本。举例来说，2019 年初，IBM X-Force IRIS 曾协助一家全球化制造公司应对数据泄露事件，一开始勒索软件只是感染了 IT 系统，随后逐渐蔓延至 OT 基础架构，最终导致工厂运营停摆。这次攻击不仅影响了该公司自身的运营，还在全球市场引发了连锁反应。

2019 年为客户提供的 X-Force IRIS 安全评估强调了 OT 系统的易受攻击性，这些系统经常会使用遗留软件和硬件。保留那些无法再修补且充斥着早已公之于众的旧漏洞的生产系统，就意味着：即便 OT 系统并非面向网络，未经修补的 OT 系统也很容易成为牺牲品。在攻击者找到第一个落脚点之后，如果发生横向移动，就可以从网络内部访问这些系统，而且通过相对简单的漏洞利用技巧即可实施破坏活动。

尽管图 1 中显示的 ICS 网络攻击从 2019 年 10 月初以来呈现下滑趋势，但 X-Force 预计，随着威胁实施者不断针对全球范围内的工业网络发起新的活动，针对 OT/ICS 发起的攻击在 2020 年会继续增加。IBM X-Force 的漏洞数据库显示，2019 年新增了 200 多个与 ICS 相关的 CVE，针对 ICS 的威胁在 2020 年也会继续保持增长态势。

X-Force 预计，随着世界各地的威胁实施者对工业网络不断发起新的活动，针对 ICS 发起的攻击在 2020 年会继续保持增长势头。

遭泄露的记录数量大幅增加

泄露记录的数量在 2019 年大幅飙升，外泄记录数已超过 85 亿条 - 相比 2018 年，同比增长三倍以上。造成这种大幅飙升的“罪魁祸首”，是由于错误配置导致的记录泄露同比增长了近十倍。这些记录占到了 2019 年数据泄露数量的 86%。这与我们 2018 年报告的数字有着很大出入，当时我们监测到，因为错误配置而泄露的记录数量比 2017 年减少了 52%，这些记录数量尚未占到总记录的一半。

值得注意的是，2019 年错误配置事件的数量实际上比上一年减少了 14%。这一事实反映了一个问题：如果确实发生了错误配置，2019 年受影响记录的数量会显著增加。近四分之三的泄露中，有超过一亿条遭泄露记录是由于错误配置事件所致。在专业服务行业发生的两起错误配置事件中，每起事件泄露的记录数量都高达数十亿条。

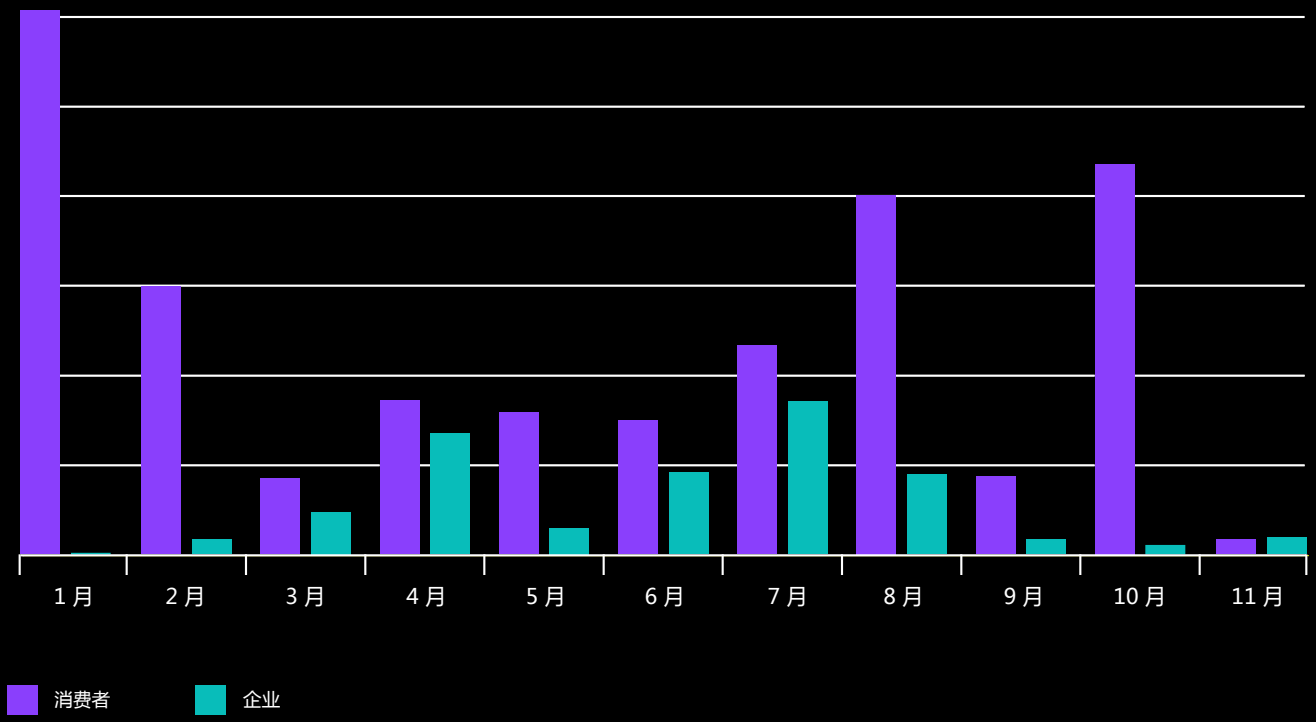
各行业丢失记录的数量大幅增加，凸显了数据泄露不断攀升的风险，即便那些通常不会视作主要目标的行业内的组织也是如此。

2019 年泄露的记录数量

85 亿条

图 2：
针对消费者与企业 IoT 的攻击

2019 年消费者与企业 IoT 每月遭受的攻击量（来源：IBM X-Force）



针对 IoT 设备的攻击目标涵盖企业领域

2020 年，接入互联网的设备将超过 380 亿台，物联网 (IoT) 威胁格局已逐渐明朗，已成为威胁消费者和企业级运营的威胁媒介之一，它们通常会使用相对简单的恶意软件和自动化（通常是基于脚本的）攻击。

在用于入侵 IoT 设备的恶意代码的范围内，IBM X-Force 研究团队在 2019 年跟踪了多次 Mirai 恶意软件活动，这些活动都有一个明显的趋势：它们将攻击的矛头从消费性电子产品转向了企业级硬件，这是我们在 2018 年并未监测到的活动。黑客可以将联网的受感染设备作为中转站，以伺机在组织内“安营扎寨”。

Mirai 是一款“作恶多端”的 IoT 恶意软件，从 2016 年以来，黑客们便一直利用这款软件制造大规模破坏，它会感染大量物联网设备并将它们用在分布式拒绝服务 (DDoS) 攻击中。通过分析 2019 年的活动，我们发现，自 2018 年以来，使用 Mirai 恶意软件的战术、技术和程序 (TTP) 发生了显著的变化，2019 年，它们的攻击目标除了消费性电子产品之外，还增加了企业硬件。

深入研究 2019 年对 IoT 设备造成影响的攻击之后，我们发现命令注入 (CMDi) 攻击十分猖獗，这些攻击中包含用于下载恶意有效负载的指令，以攻击不同类型的 IoT 设备。大部分此类注入攻击都是通过脚本自动发起，脚本会扫描并试图大规模感染设备。如果作为攻击目标的 IoT 设备容易受到此类注入攻击，就会下载并执行恶意程序，而且会将设备迅速拉入庞大的 IoT 僵尸网络。这些攻击之所以能够得手，一个最常见的“幕后推手”就是 IoT 设备使用了较弱或默认的密码，哪怕是一次微不足道的字典式攻击也能轻易猜出密码。

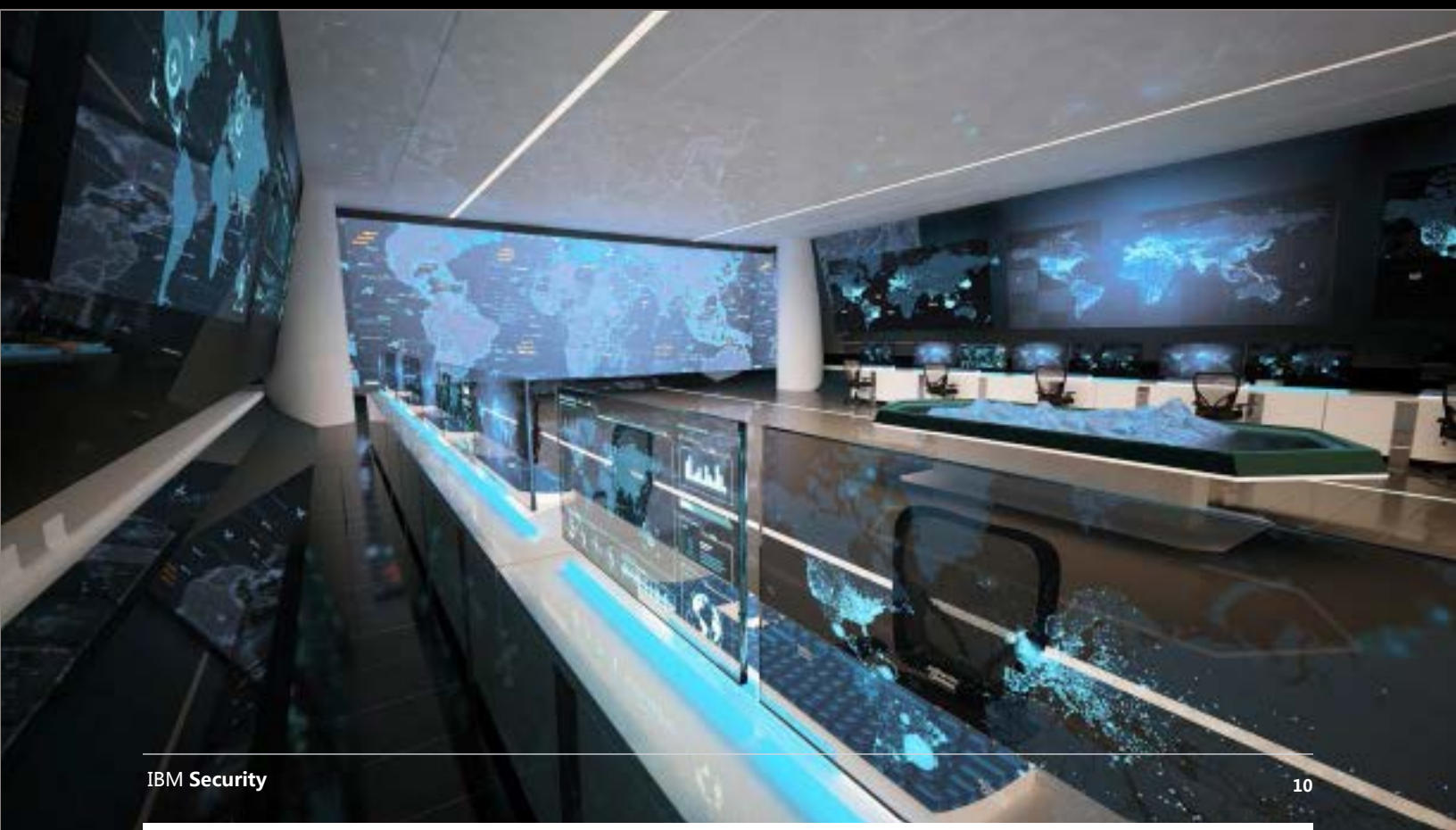
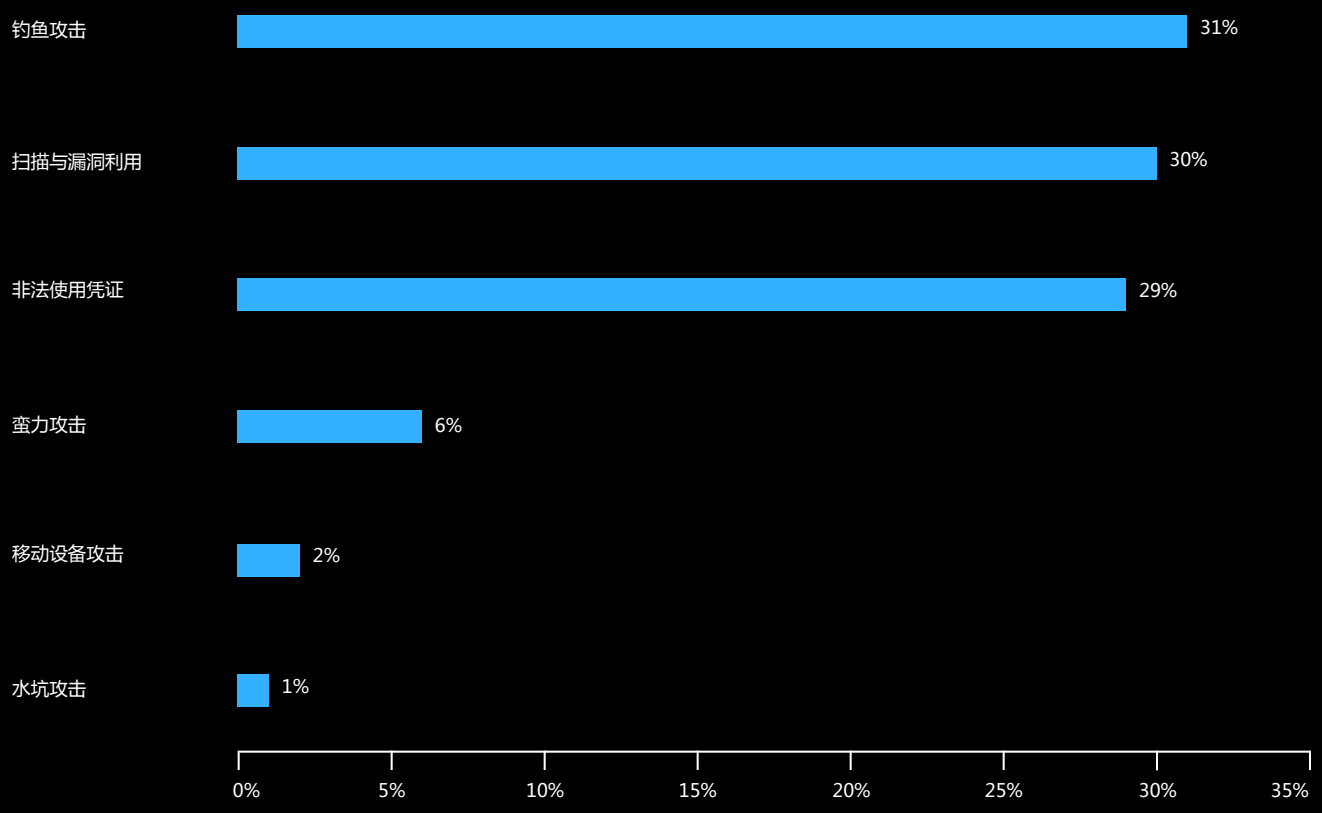


图 3：
主要的初始访问媒介

2019 年最主要的 6 种初始攻击媒介的细分，以百分比显示的 6 种访问媒介（来源：IBM X-Force）

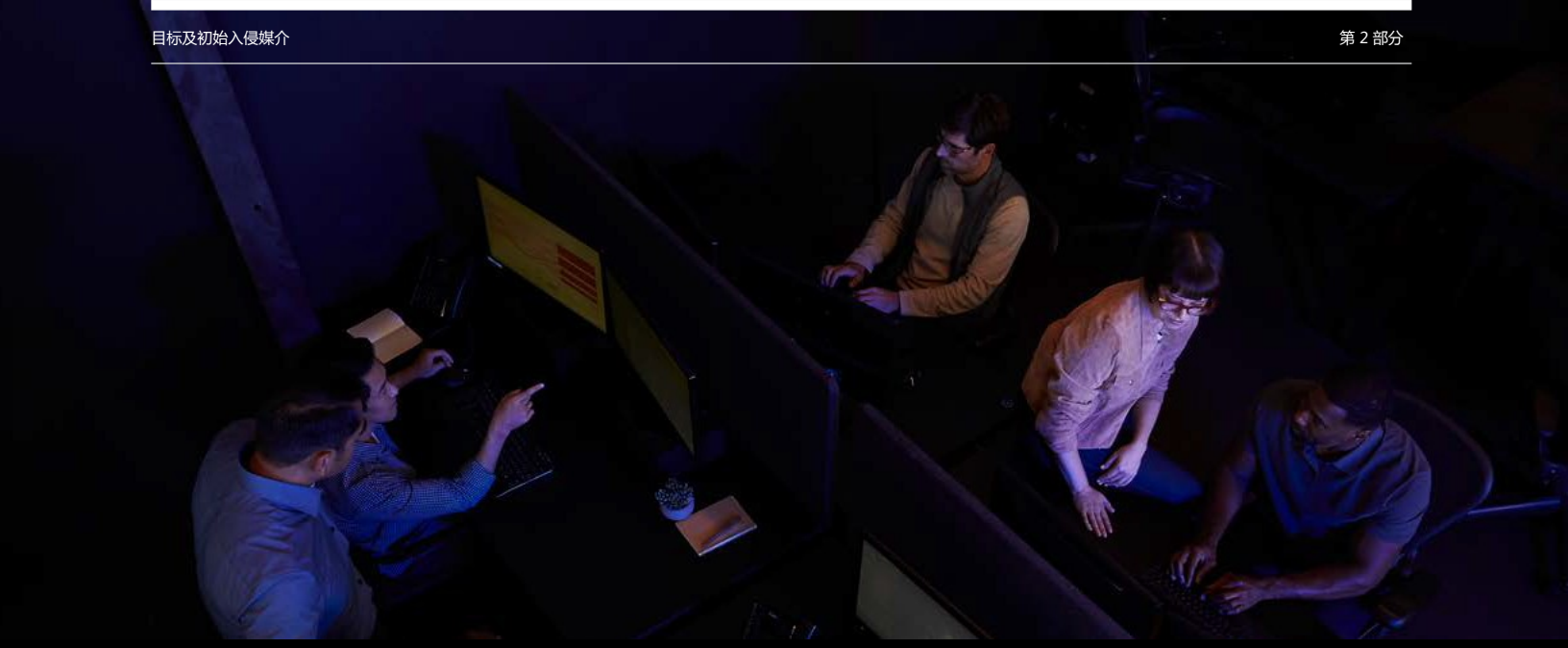


在 2019 年的网络攻击中，钓鱼攻击成为头号初始访问媒介

IBM X-Force IRIS 拥有广泛的事件响应能力，能够对攻击方法和动机提出宝贵的洞察力。

2019 年，钓鱼攻击是初始访问最常用的媒介，占比为 31%，但与 2018 年相比有所下降，当时钓鱼攻击占到了总数量的近一半。[1]

1 2019 年 X-Force 威胁情报指数报告显示，在 X-Force IRIS 分析的攻击中，有近三分之一 (29%) 的破坏活动是通过钓鱼电子邮件发起的。此后已对该数字进行了调整，因为几起事件在披露之后有更多证据浮出水面，使这一比例在 2018 年增加到 44%。



最值得注意的是， 2019 年，攻击者越来越多地开始扫描目标环境，以发现可以利用的漏洞，事件响应人员发现，有 30% 的事件使用了这一伎俩，而在上一年，此类攻击仅占总事件的 8%。

威胁实施者可以选择的扫描和利用的对象有很多，IBM X-Force 跟踪了 150,000 多个已公开披露的漏洞。一些老奸巨猾的对手会开发零日漏洞，通过依赖比此类零日漏洞更频繁发生的已知漏洞，对手不需动用一兵一卒来拟定新的 TTP 即可初步站稳脚跟，利用他们最有杀伤力的武器来侵入防御能力最强的网络。此外，攻击者会寄希望于那些没有更新其补丁应用程序的组织，尽管有些漏洞的补丁程序在很久前便已推出。举例来说，自发生首例 WannaCry 感染并广泛推广补丁程序 (MS17-010) 之后的两年多内，WannaCry 感染现象仍然层出不穷。

威胁实施者使用之前获取的凭证来访问目标组织，即使用被盗凭证实施的攻击以 29% 的比例占到了近三分之一。这些凭证通常是从第三方网站窃取，或是通过向目标组织发起的钓鱼攻击而获得。威胁实施者可以使用被盗凭证混进合法流量中，要发现它们的踪迹就变得难上加难。

蛮力攻击与上一年相比有所下降，以 6% 的占比在所有事件中排名第四，紧随其后的是 BYOD 设备 (2%)，它是进入目标组织的初始访问点。

X-Force 研究人员发现，威胁实施者的活动在 2019 年 6 月份和 7 月份有显著的增长，这段时期的事件数量超过了 2019 年全年的总数。尽管活动数量突然暴增的原因不得而知，垃圾邮件在夏季也似乎更加活跃，其数量在 2019 年 8 月达到峰值。
原因可能是威胁实施者变得更加招人耳目，更容易被发现，又或者是因为威胁实施者战略或工具发生改变而产生了大量活动。但出现短暂的活动峰值不太可能是因为有新的威胁实施者进入市场，因为若出现新的威胁实施者，势必会让活动持续增加，而不是这般昙花一现。

恶意软件趋势

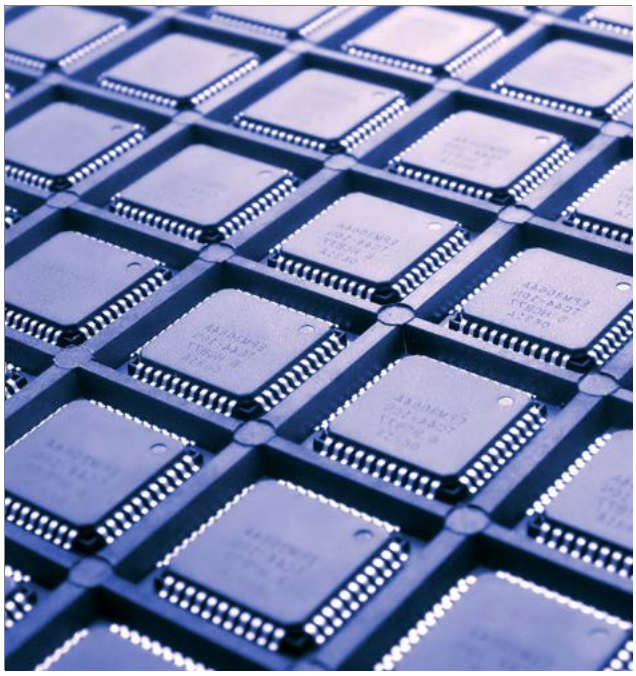
破坏性恶意软件攻击的数量大幅增加

IBM X-Force IRIS 调查发现，2019 年，破坏性恶意软件攻击变得更加频繁，并且无论是攻击的地理范围还是规模都有所增加。

破坏性恶意软件是网络犯罪分子和民族国家威胁实施者常用的伎俩，它能够使受影响的系统无法运行，并让重建变得困难重重。大多数破坏性恶意软件变体都会通过删除或覆盖对操作系统运行能力而言至关重要的文件，来达到破坏的目的。在少数情况下，破坏性恶意软件可能会向工业设备发送量身定制的消息以引发故障。
在我们对破坏性恶意软件的定义中还有一类勒索软件，它能够清除机器上的数据或对机器上的数据进行不可逆的加密。

2018 年下半年与 2019 年下半年，2019 X-Force IRIS 处理了相同数量的破坏性攻击，不难看出，这种潜在的灾难性恶意软件会继续让组织面临风险。

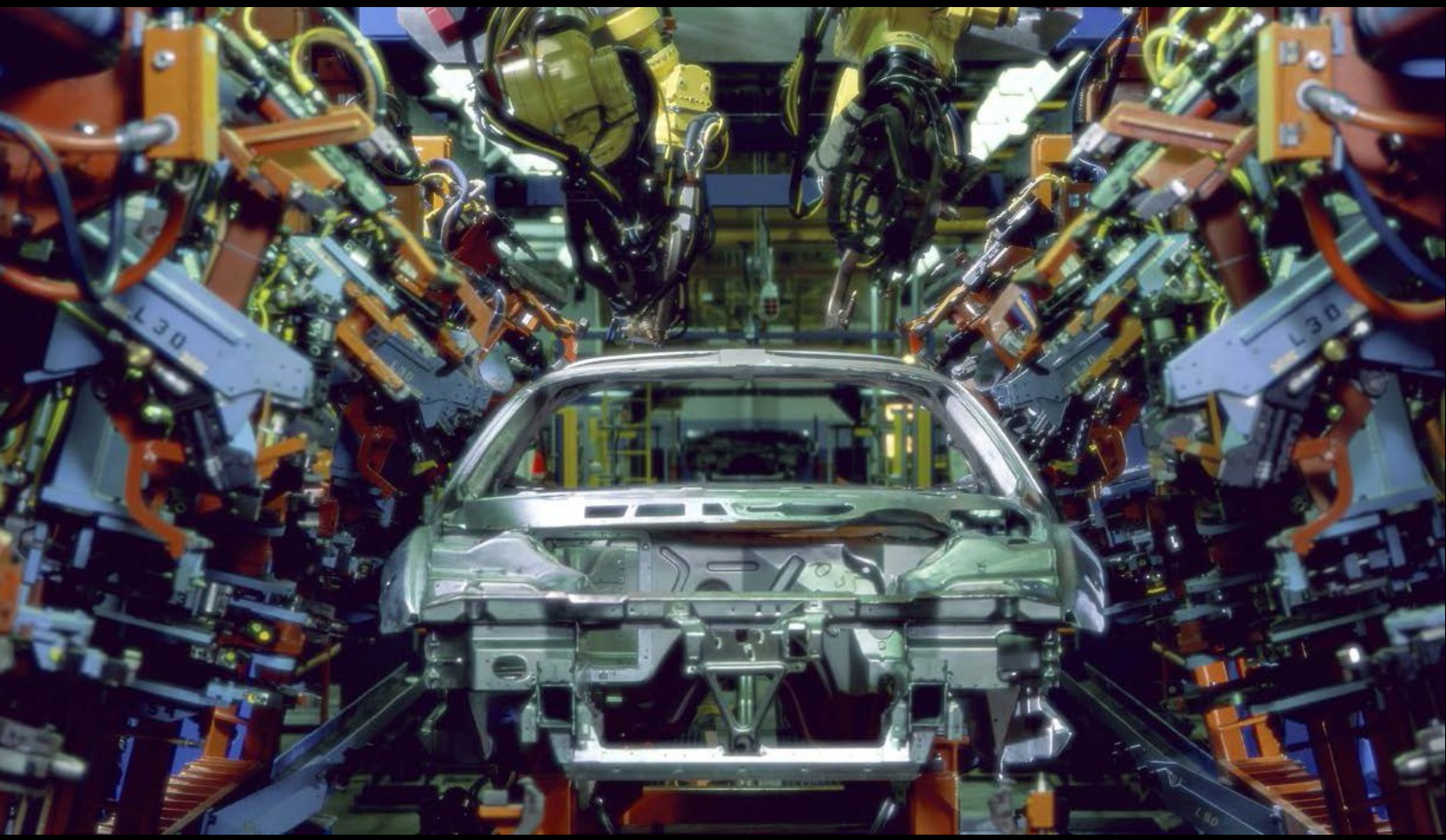
从历史上看，破坏性攻击通常来自民族国家对手。但我们监测到这么一种趋势：越来越多受经济利益驱动的勒索软件会在攻击中使用破坏性元素，以变体 LockerGoga 和 MegaCortex 为例，它们在 2018 年底和 2019 年初首次发动了破坏性攻击。



破坏性攻击造成的损失平均在 2.39 亿美元左右，是数据泄露平均成本的 60 倍以上。

2019 年底，X-Force IRIS 发现了一种名为 ZeroCleare 的新型破坏性恶意软件。这款删除式恶意软件的攻击目标是中东的能源行业，IBM 认定它来自隶属于伊朗的 APT 集团 ITG13[2]（也被称为 APT34/OilRig）。

X-Force IRIS 预计，破坏性恶意软件攻击会让公司付出惨重的代价，大型跨国公司在每起事件后支付的平均成本高达 2.39 亿美元。此成本估算是 2019 年数据泄露平均成本的 60 倍以上。与专门窃取或暴露数据的数据泄露的不同之处在于，破坏性攻击通常会让受害组织四分之三甚至更多的设备毁于一旦。



2 ITG 是 IBM Threat Group 的缩写，我们在“最常受到攻击的行业”中会进一步探讨这一术语。X-Force 使用 ITG 名称，并在 ITG 名称后面的括号中指明威胁团伙的备用名称。

勒索软件和加密货币挖矿软件在 2019 年猖獗肆虐

恶意软件变体以及使用恶意软件发动的攻击数量在一年内起起伏伏，但是尽管如此，对那些不容忽视的威胁类型的了解会帮助组织更好地管理风险。

2019 年上半年，我们监测到的攻击中约有 19% 与勒索软件事件有关，而 2018 年下半年这一比例仅为 10%。2019 年第 4 季度，勒索软件活动与上一年第 4 季度相比增加了 67%。2019 年，X-Force IRIS 响应了 5 大洲 12 个国家或地区的勒索软件活动，这些活动涉及 13 个不同的行业。

这种激增可能是由于 2019 年威胁实施者以及针对不同组织发起的活动数量不断增长导致的。值得注意的是，受到勒索软件攻击的除了市政和公共机构之外，还有地方政府机构和医疗保健提供者。对这些组织发起的攻击常常会令他们措手不及，只得支付赎金，并且在某些情况下，因为会威胁到公共安全和生命，他们还要承受巨大的压力从攻击中迅速恢复。

X-Force 数据显示，在勒索软件攻击活动中，2019 年的头号攻击媒介是利用 Windows SMB 协议中的漏洞通过网络进行传播。这一伎俩曾在 WannaCry 攻击中用过，占到了已监测到的攻击尝试的 80% 以上。

与 2018 年第四季度相比，2019 年第四季度的勒索软件活动增加了 67%。

图 4：
多阶段勒索软件感染

分多阶段入侵的勒索软件攻击（来源：IBM X-Force）

SMB 协议带有安全漏洞，针对该协议的攻击可以自动发起，这使它成为了威胁实施者的一种低成本攻击选项，且更易于扩展攻击范围，可以在一次攻击中影响尽可能多的系统。

威胁实施者还经常使用 Emotet 和 TrickBot 等常见的商用下载器，在目标系统上执行勒索软件。这种手段经常会利用 PowerShell 下载恶意软件，并利用 PSExec 或 Windows Management Instrumentation (WMI) 等本机功能进行传播，从而进一步加大了检测难度。

攻击者会分多个阶段来感染用户，而不是利用勒索软件直接命中目标，这样一来，攻击者能够更好地掌控攻击，逃避控制措施和检测，并埋下勒索软件操作的种子，感染尽可能多的设备，从而迫使受害者就范，甘愿支付赎金。这种耐心和筹谋带来了丰厚的回报：短短五个月内，Ryuk 攻击就为他们的犯罪集团积敛了 370 多万美元的不义之财。在另一个实例中，Ryuk 运营商对美国养老院发动攻击并索要 1400 万美元的赎金。

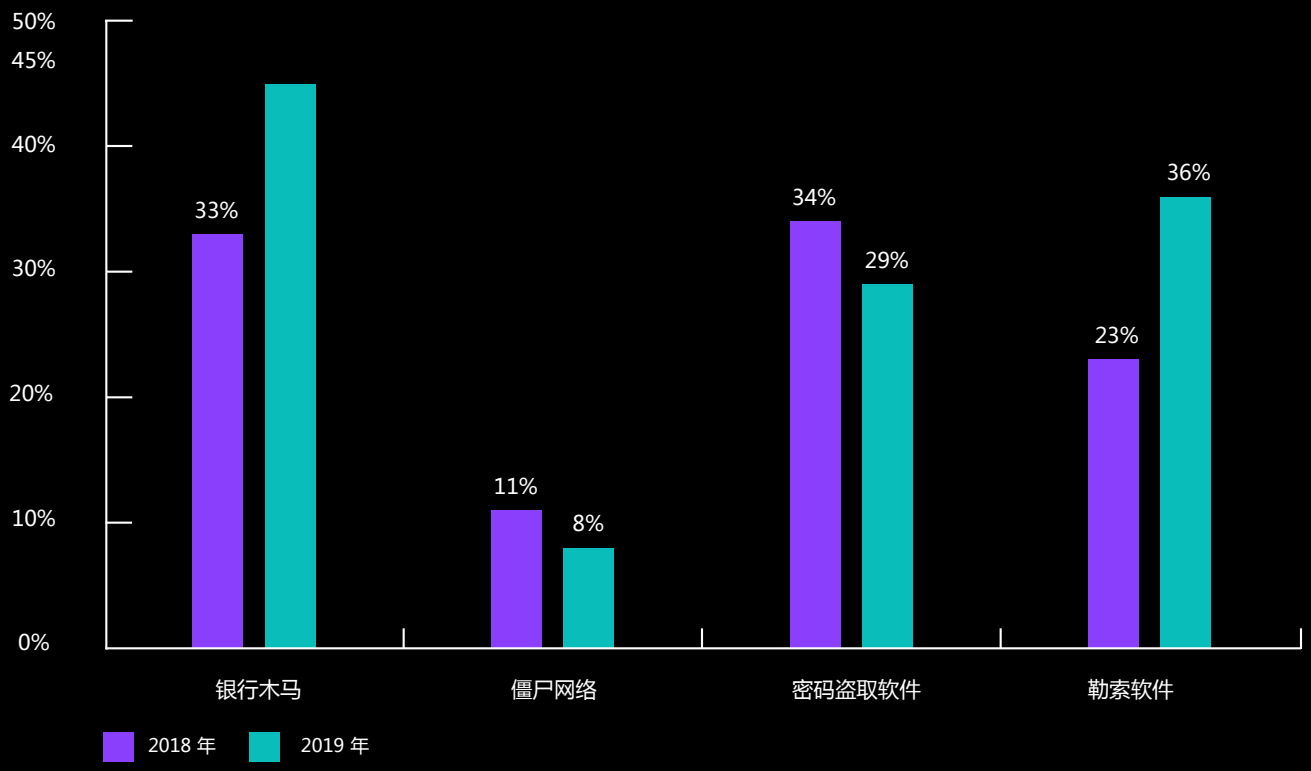
勒索软件并不是 2019 年唯一一款异军突起的恶意软件。加密货币挖矿代码是 2019 年另一款格外猖獗的恶意软件。

据 X-Force 遥测，加密采矿活动在 2019 年中期飙升至前所未有的水平，6 月份的活动数量几乎已经超过了全年所有的其他加密挖矿活动的总和。

尽管恶意软件趋势随着僵尸网络操作者的动机和资源起起伏伏，但是这种激增却可能与 Monero 的价值飙升三倍有关 - Monero 是恶意软件矿工经常使用的一种加密货币。

图 5：
恶意软件遗传代码创新

按类别划分的新（之前未监测到）代码百分比，2018-2019 年（来源：Intezer）



2019 年恶意软件代码演变方面的头号创新选手

通过借鉴 X-Force 之前在检测新恶意软件变体方面的协作，Intezer 利用其遗传恶意软件分析技术揭示了所有软件代码的遗传来源，从中发现代码相似性和代码复用，以测量恶意软件的“升级换代”。这种测量与威胁实施者投资开发新代码的力度相当，从中可以看出对手也在积极扩大其威胁能力并竭力逃避检测。

Intezer 提供的数据显示，2019 年，威胁实施者主要侧重于开发和升级银行木马和勒索软件的代码库，同时还在不遗余力地修改和制造加密挖矿恶意软件毒株。

报告的这一部分由 IBM X-Force 和 Intezer 研究人员合作完成。Intezer 针对恶意软件的二进制代码执行了遗传分析。

2019 年，银行木马在新代码中所占比例最高 (45%)，勒索软件紧随其后 (36%)。就过去经验看来，IBM 发现威胁实施者对那些可以有效攻击企业用户的恶意软件类型保持着浓厚的兴趣，而且不断对其进行投资，这表明这些恶意软件家族可能会在 2020 年将企业作为攻击目标。如果他们不持续改进，银行木马和勒索软件运营商将会陷入绝境，因为恶意软件会更快地被检测出来并降低攻击的长期投资回报。

2019 年，威胁实施者集中精力开发和升级银行木马和勒索软件的代码库。

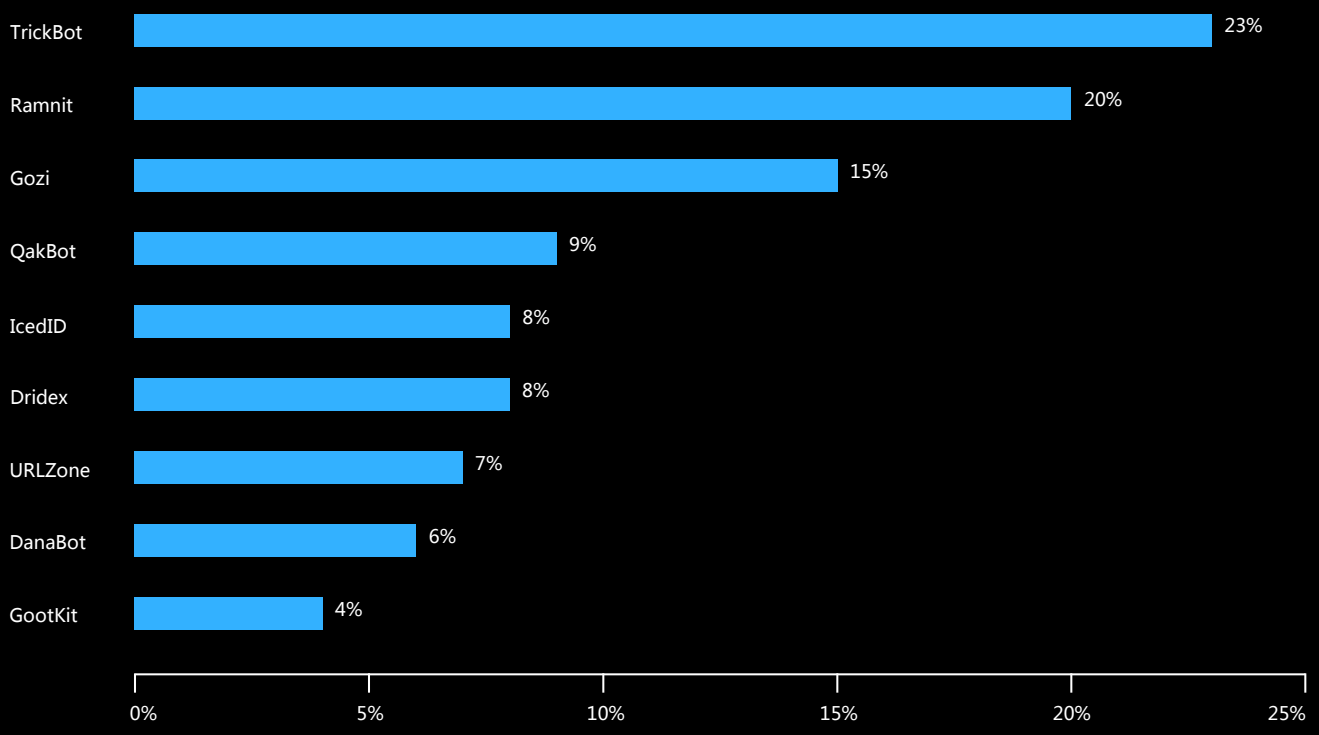
2019 年，加密货币挖矿软件的创新能力有所下降，但挖矿活动量仍居高不下，这表明威胁实施者会继续开发新版本的加密货币挖矿软件，但也更加依赖之前的代码。根据 IBM 的经验，这些简单的恶意软件代码往往会依赖其他一些无恶意的“前辈”，例如 XMRig，他们对 XMRig 进行修改之后便能以非法方式将财富收入囊中。不过，他们也会出于不同的目的编写新的挖矿程序，例如对 IoT 设备收割财富，或者在另一个极端 - 对感染服务器收割财富，服务器的 CPU 功耗要高于小型设备和单个 PC。

相比之下，一般的僵尸网络恶意软件 (11%) 每年的代码创新较少，这表明威胁实施者减少了在修改其功能方面的投资。IBM 发现这些类型的代码是通过垃圾邮件或恶意广告推送给用户的。一般僵尸网络恶意软件的主要作用是在受感染的设备上站稳脚跟，但它们的功能仍然极其有限，这也就解释了它们的代码进化级别为何一直较低。

2020 年，从这些代码创新趋势中可以看出某些需要更多投入来识别和遏制的恶意软件。

图 6：
主要的银行木马家族

2019 年主要银行木马家族细分，以百分比显示九大木马家族（来源：IBM X-Force）



银行木马与勒索软件 - 一段越发危险的“联姻”

十多年前，随着宙斯木马之类的恶意软件的兴起，金融恶意软件成为了一个主流问题，宙斯木马是当时的网络犯罪领域第一个普遍可用的商业银行木马。回顾 2019 年金融犯罪形势，从中可以看出主要银行木马犯罪团伙的明显趋势：这些恶意软件僵尸网络越来越多地被用于敲开攻击目标的大门，然后实施高回报的勒索软件攻击。

2019 年该类别中最活跃的特洛伊木马家族的图表与我们在 2018 年度综述中生成的图表非常相似。TrickBot、Gozi 和 Ramnit 占据了前三名的位置。这些特洛伊木马由有组织的团伙负责运营，这些团伙为其他网络犯罪参与者提供不同的商业模式，例如僵尸网络租用服务计划以及通过沦陷的资产进行传播。

到目前为止，运营 TrickBot 的团伙是 2019 年网络犯罪领域最活跃的犯罪软件团伙。这种活动表现在多个不同的方面：

- 代码更新和修复的频率（代码、版本和功能演变）

- 入侵活动的频率和规模

- 攻击活动的频率和数量

2019 年发起高风险勒索软件攻击并成为头条新闻的团伙，正是 2015 年在网络犯罪领域引入高风险电信欺诈活动的始作俑者。在某种意义上来说，总体战略基本一样，只对具体策略做出了一些改动：瞄准企业牟取更丰厚的回报。

此外，2019 年底的报告显示，一直以来专门大规模窃取支付卡数据的 ITG08 (FIN6) 也在努力让自己的 TTP 实现多样化发展。它现在的工作重心是要在企业网络上部署勒索软件。收集、销售或使用窃取的卡数据，需要投入大量时间和精力才能变现，而勒索软件攻击却能不费吹灰之力便将数百万美元收入囊中，这一巨大的利润诱使更多犯罪团伙去使用勒索软件并走上网络敲诈勒索的道路。

演变成勒索软件的主要银行木马示例：

Dridex
之前是将 LokiBot 传播到用户设备上，现在是在企业网络上部署 BitPaymer/DopplePaymer。

GootKit
在企业网络上部署 LockerGoga 的嫌疑分子。LockerGoga 在 2019 年初出现，已经成为向企业发起严重攻击的中坚力量。

QakBot
在企业网络上部署 MegaCortex。

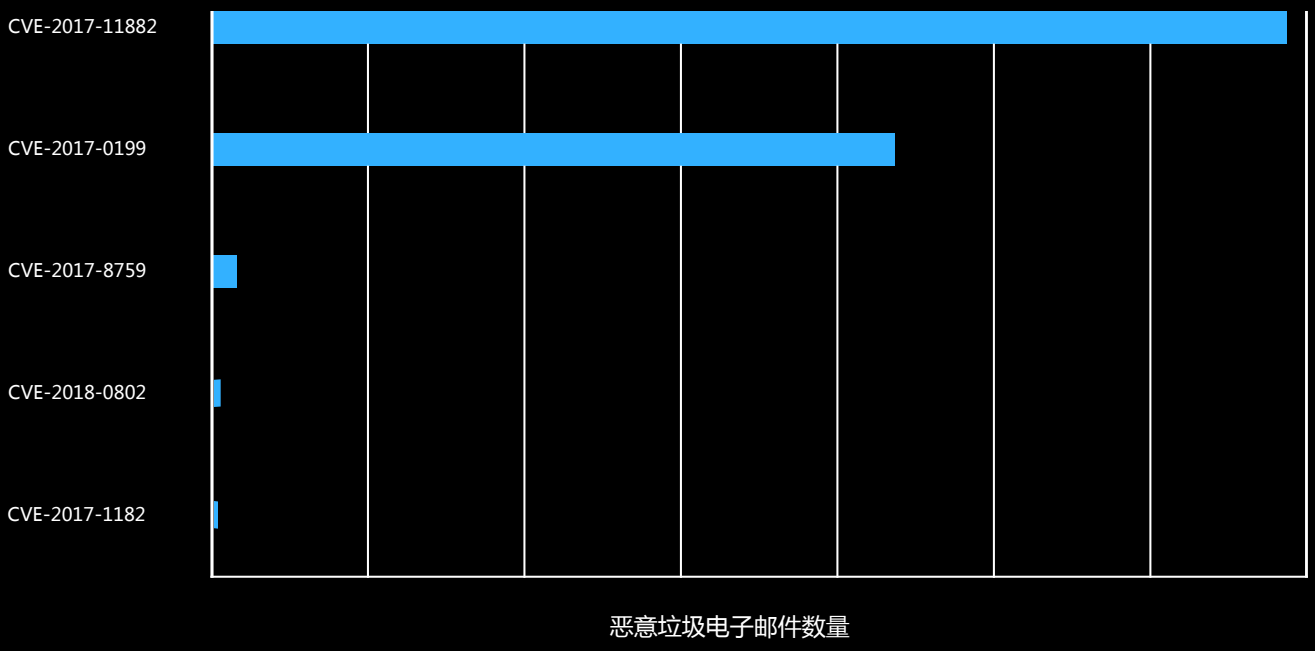
TrickBot
在企业网络上部署 Ryuk。

垃圾邮件和钓鱼攻击的趋势

图 7：

恶意垃圾邮件中利用的主要漏洞

2019 年恶意垃圾邮件附件中利用的主要漏洞细分，按数量划分（来源：IBM X-Force）



2017 年的漏洞在 2019 年的垃圾邮件攻击中继续“发光发热”

IBM X-Force 每天都会运行世界各地的垃圾邮件陷阱，并监控数以千万计的垃圾信息和钓鱼攻击电子邮件。我们的团队和技术人员会分析数十亿计的网页和图像，以检测欺诈活动和品牌滥用。

X-Force 对全球垃圾邮件活动分析后得出结论，垃圾电子邮件会继续使用有限的漏洞，尤为值得关注的只有两个 CVE：2017-0199 和 2017-11882。这两个漏洞均为已修补的漏洞，在威胁实施者尝试通过垃圾邮件活动利用的漏洞中占比近 90%。这些 CVE 都会影响 Microsoft Word，并且除了打开一份设置了陷阱的文档之外，根本无需用户操作。

我们的事件数据显示，2019 年攻击者利用这两个漏洞的频率比任何其他 Microsoft Word 远程代码执行漏洞的使用频率高出近 5 倍。

尽管这两个漏洞是大量垃圾电子邮件的常客，但并不能因此说明它们在攻击用户方面有多么成功。也就是说，垃圾邮件常常是一个数字游戏；只要数量足够，即便是一次偶然的成功也能为威胁实施者带来收益。因为许多用户甚至是组织都不能做到及时修复问题，因此攻击者仍可使用原来的漏洞对设备发起攻击。

原来的漏洞长盛不衰的原因有很多，例如可以轻松植入、可以使用免费的文档生成器、具有持续的效力或者是因为它们的多功能性，可以投放各种恶意的有效负载等等。

原有漏洞的持续使用凸显了恶意活动的长尾效应，还可以看出，在披露和补丁发布数年后仍可利用重大漏洞攻击用户。

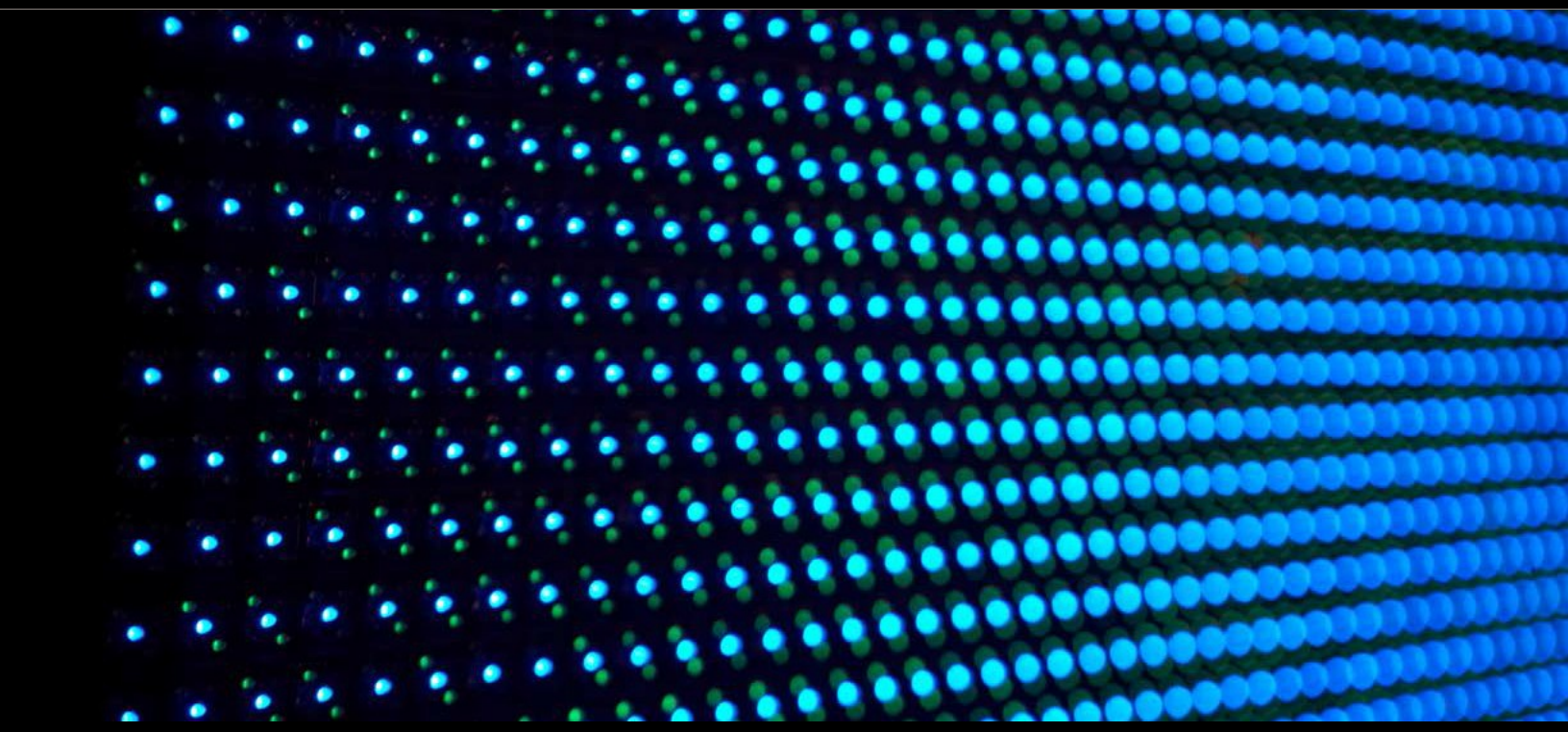
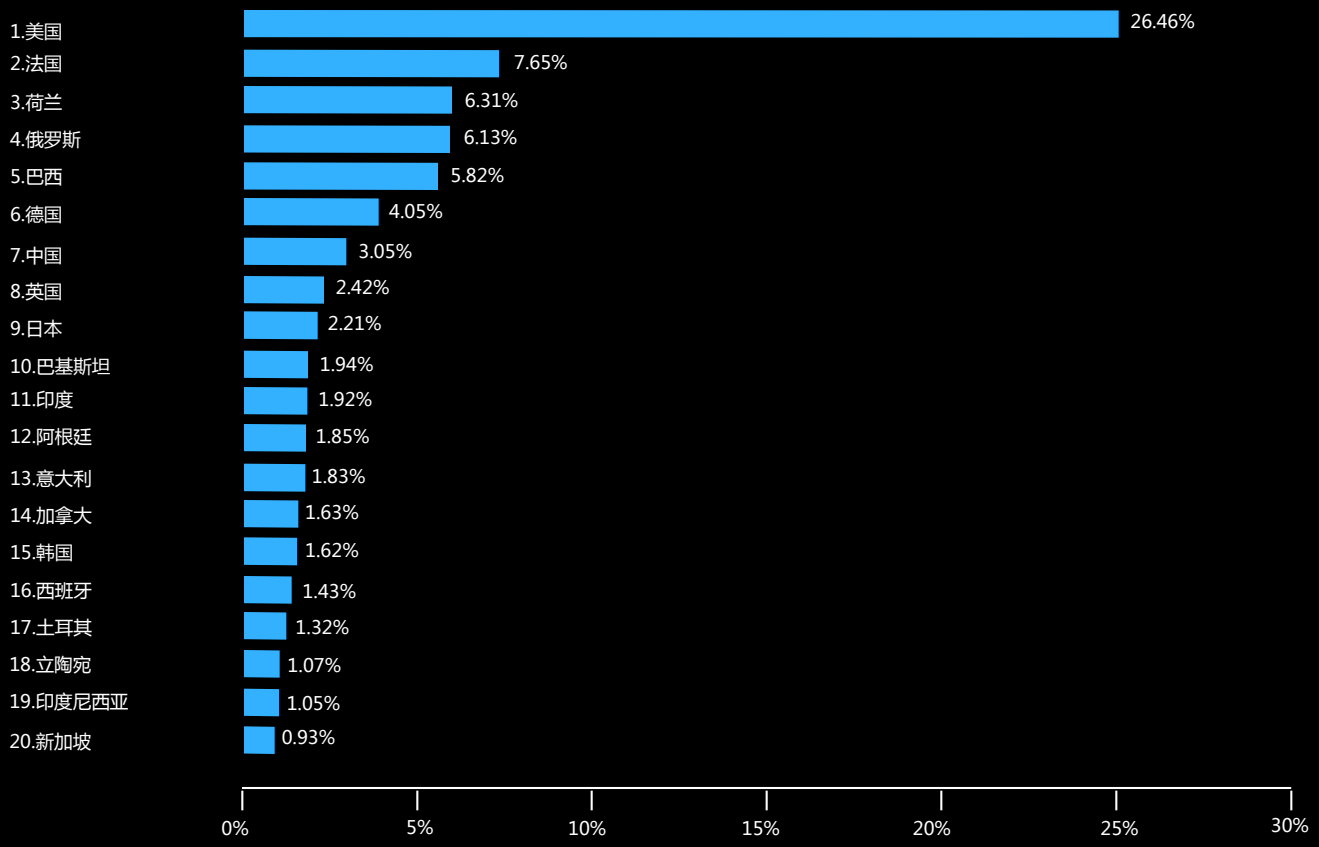


图 8：

托管垃圾邮件 C2 的 20 个主要国家或地区

2019 年按全球垃圾邮件命令与控制 (C2) 服务器份额排名前 20 位的国家或地区。（来源：IBM X-Force）



西方的垃圾邮件僵尸网络殃及全球

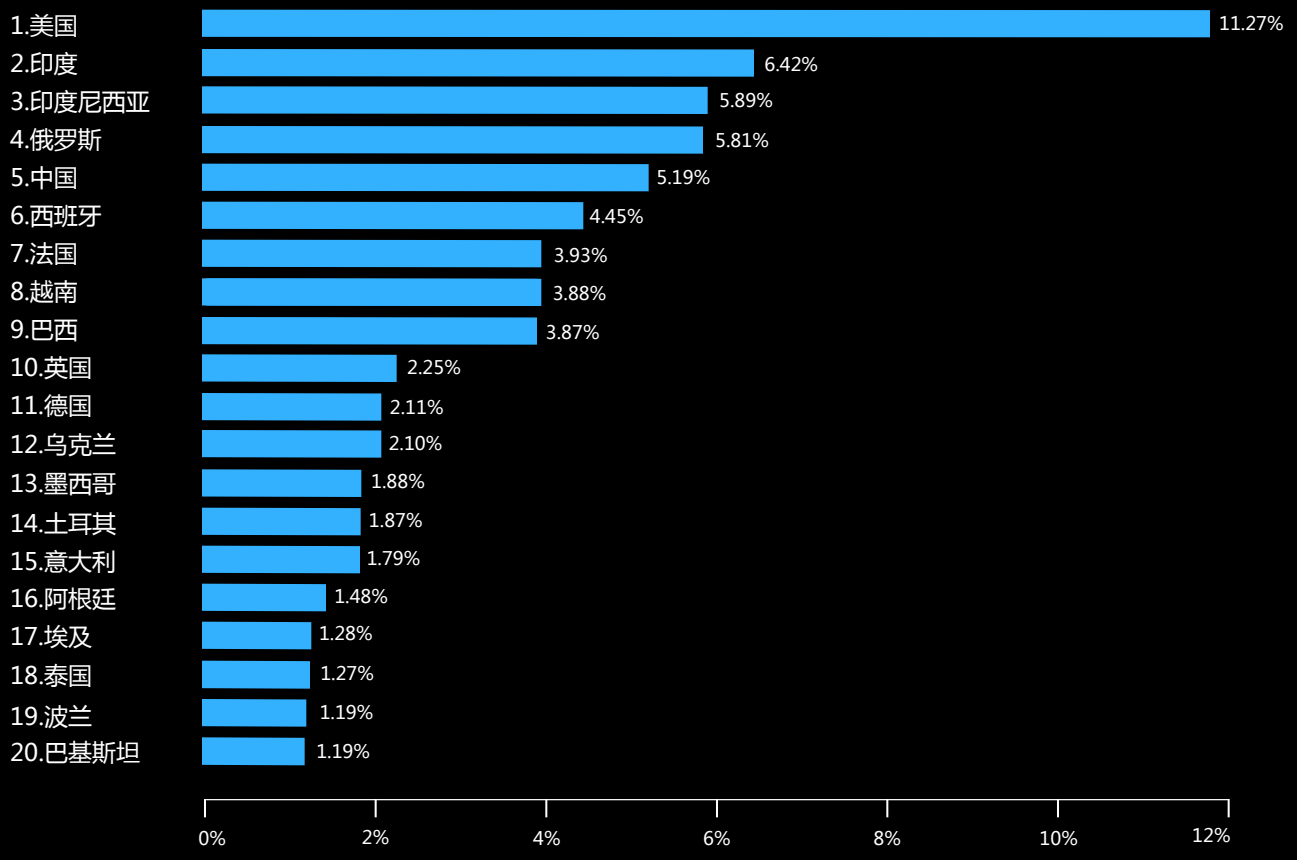
IBM X-Force 通过垃圾邮件僵尸网络的研究，深入了解了各种地理位置特定的数据点，这些数据点与垃圾邮件僵尸网络的命令和控制 (C2) 基础架构密切关联。我们探寻的其中一个参数就是托管僵尸网络 C2 的地理位置。2019 年，我们发现 C2 主要托管在北美和西欧国家，占 2019 年监测到的所有 C2 实例的一半以上。剩余的 C2 托管分散在几个较大的区域。

在许多情况下，垃圾邮件僵尸网络 C2 基础架构都托管在受影响的服务器上，并且北美和欧洲服务器的使用都符合一个共识，即这些国家或地区通常拥有更一致的服务器正常运行时间。此外，网络犯罪分子更愿意攻击本地资源，当这些服务器中的流量与目标地理位置的设备和网络互动时，不太可能释放危险信号。

图 9：

垃圾邮件僵尸网络受害者最多的 20 个国家或地区

2019 年按全球垃圾邮件僵尸网络客户（受害者）份额排名前 20 位的国家或地区。（来源：IBM X-Force）



按地理区域划分的垃圾邮件受害者

2019 年垃圾邮件僵尸网络受害者遍布世界各地，其中美国的受害者人数最多，紧随其后的是印度、印度尼西亚、俄罗斯和中国。攻击目标的分布情况与垃圾邮件制作者的动机一致，即通过大量垃圾邮件活动来吸引尽可能多的收件人。人口较多的国家或地区，垃圾邮件泛滥的程度自然也会更高。

已拦截的恶意域名凸显了匿名化服务的普遍性

要增加网络的安全性，使其远离线上威胁，一种常见的做法是防止用户和资产与潜在或未知的恶意域名进行通信。为了最大程度降低风险，大多数组织都将可疑的 IP 地址列入黑名单。基于这一想法，开发出在全球范围内免费提供的域名服务器 (DNS) 服务 Quad9[3]，它平均每天可阻止 1000 万个对恶意站点的 DNS 请求。

根据与 IBM Security 威胁情报相关的 Quad9 数据抽样，垃圾邮件中发现的 URL 占了可疑 DNS 请求的大部分，2019 年占所有请求的 69%。尽管与 2018 年 77% 的比例相比略有下降，但垃圾邮件 URL 仍是最重要的恶意域名类别。之所以有 8% 的下降，可能要归因于匿名化服务类别，它占到了 DNS 请求的 24%。

垃圾电子邮件仍是最奏效的方式之一，它凭借庞大的垃圾邮件僵尸网络（如 Necurs 僵尸网络），能够接触到最大数量的受害者，每天可传播数百万封垃圾电子邮件。恶意域名通常会散布恶意软件以分发勒索软件、凭证窃取脚本或指向进一步骗局的链接，并且会乔装成合法品牌或冒充人们知道的品牌来欺骗最终用户。

垃圾电子邮件中的恶意 URL 链接也是大多数受经济利益驱动的攻击者首选的方法，他们可以轻松设好骗局，或者选择地理特定的目标，即便骗局被揭穿，也不会大规模曝光。

图 10 中的图表显示了 2019 年 IBM Security 记录的恶意域名类型的分布情况。

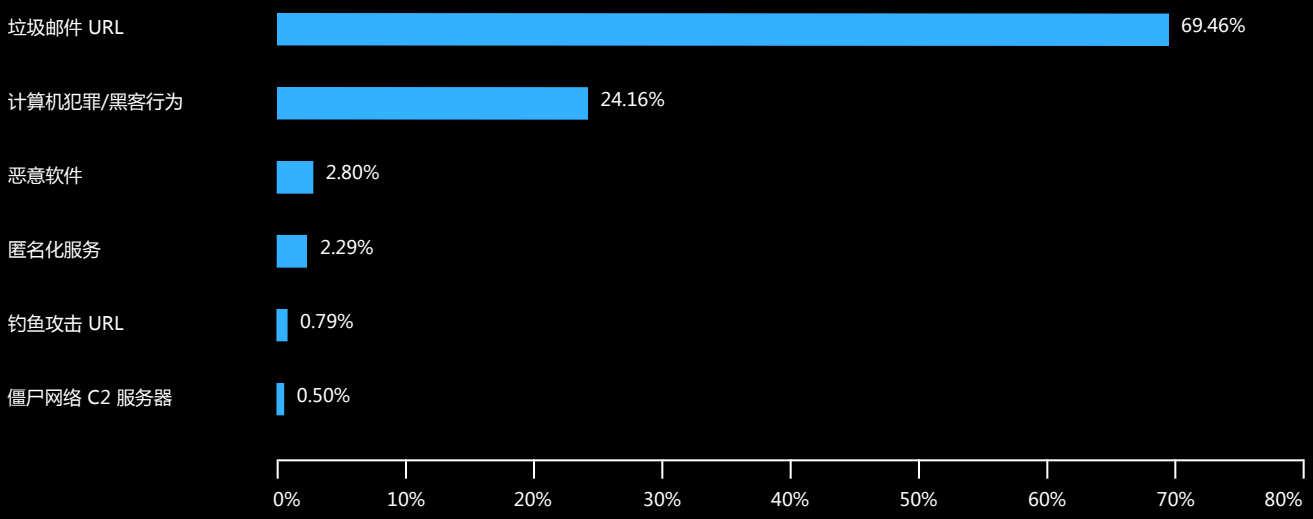
垃圾电子邮件仍是可以接触到最多潜在受害者的最有效的方式之一。

3 IBM、Packet Clearing House (PCH) 和 Global Cyber Alliance (GCA) 紧密协作，共同创立了 Quad9 并对此提供赞助。

图 10：

主要的恶意域名威胁类型

2019 年主要恶意域名威胁类型细分，以百分比显示的 6 种类型（来源：IBM X-Force 和 Quad9）



垃圾邮件 URL：
链接至与垃圾邮件活动相关的站点的域名，它通常是一种屏障，但与进一步的犯罪活动无关

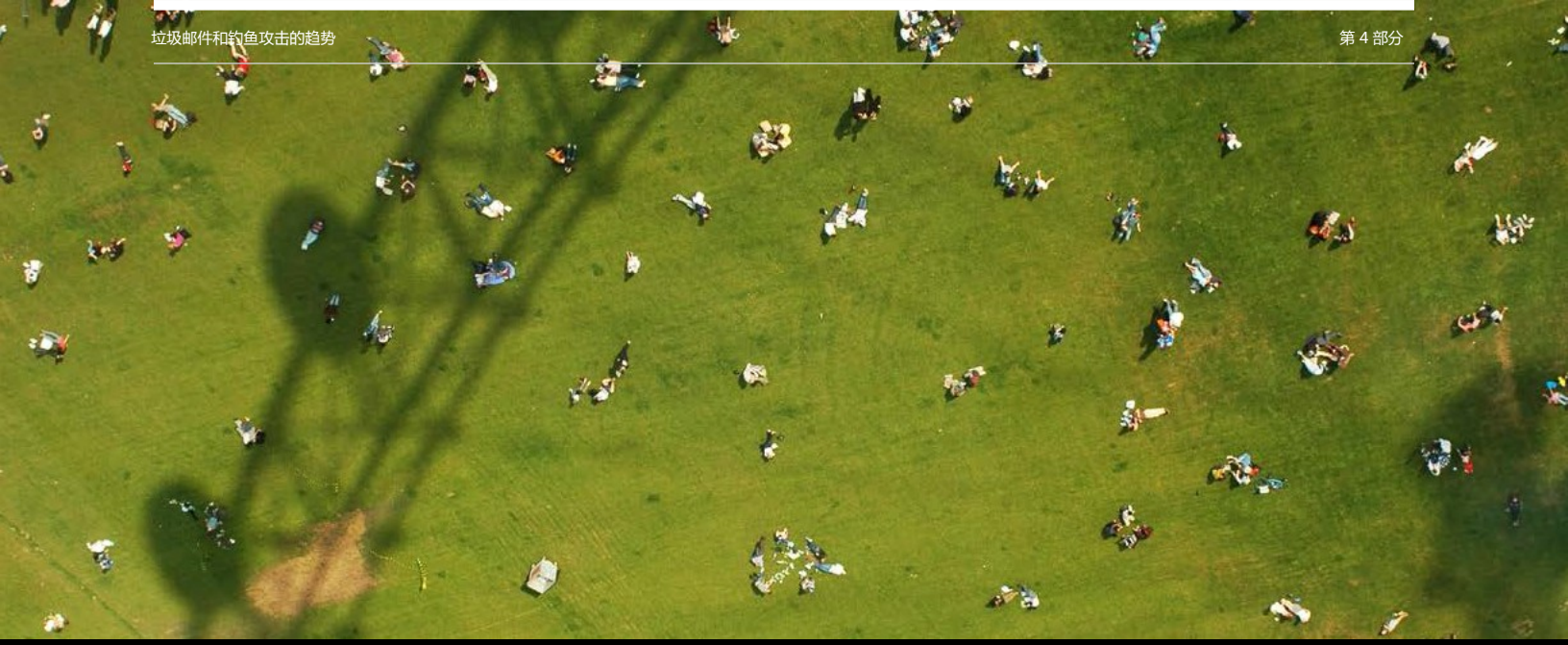
钓鱼攻击 URL：
伪装成其他合法域名，通常是试图从用户那里获取凭证数据或其他敏感信息

匿名化服务：
链接至匿名化提供商的域名，它会隐藏流量，无法查看

僵尸网络命令和控制：
链接至僵尸网络活动的域名，可能会感染访问者

计算机犯罪/黑客攻击：
明确标识为从事犯罪活动的域名，例如托管网络浏览器利用脚本的网站

恶意软件：
托管已知恶意软件的域名



Tor 之类的匿名化服务提供商，允许用户通过其他威胁实施者运营的节点来匿名处理他们的网络流量来源。尽管匿名化服务可以且经常有合法的目的，例如为用户的网络浏览活动提供更强的隐私保护，这种活动让它更难或根本不可能跟踪并拦截恶意活动。

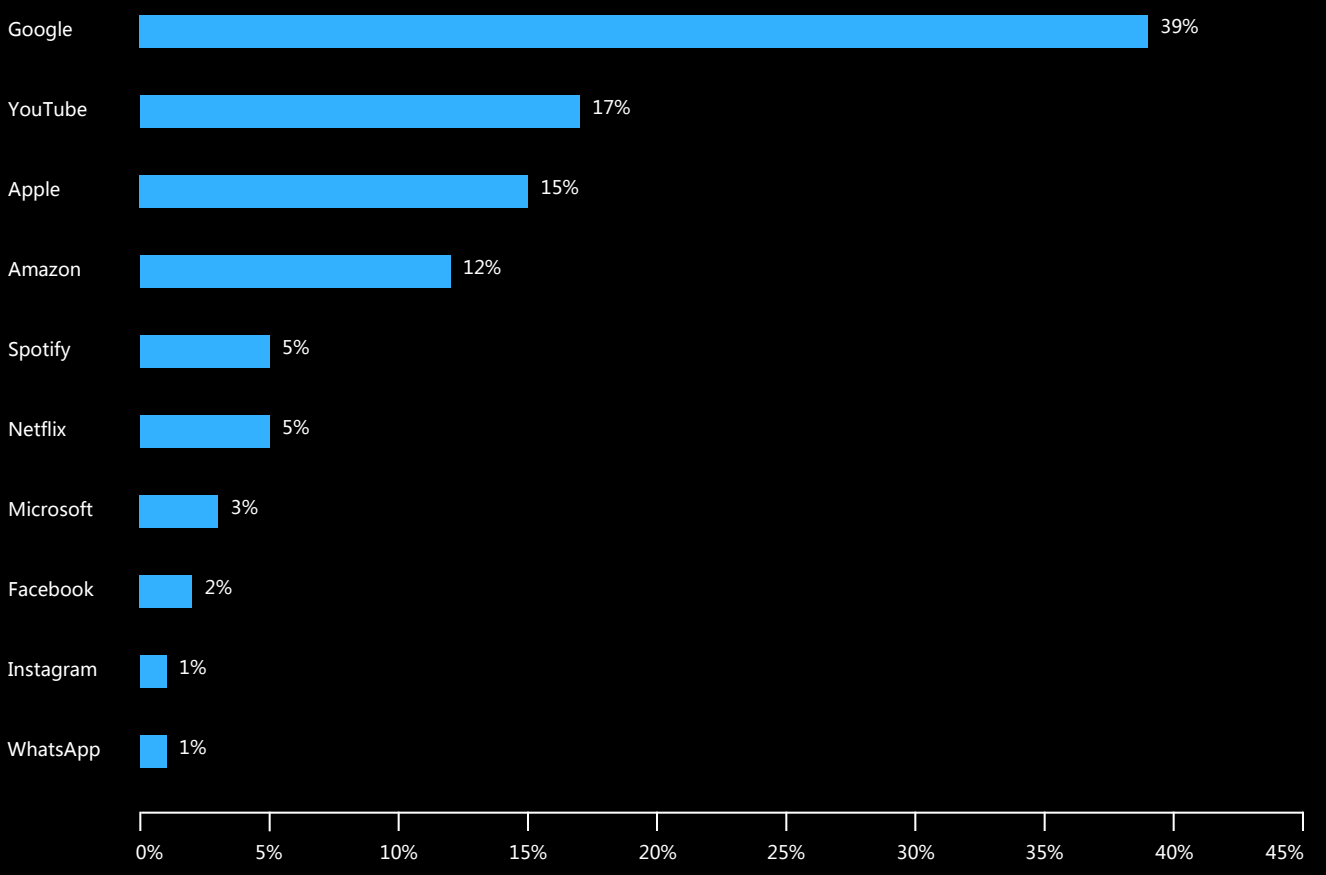
匿名化是网络犯罪分子为了掩盖其行踪而经常使用的一种伎俩，因为它可以混淆恶意链接，在不触发数据丢失保护 (DLP) 规则的情况下泄露数据，或者在锁定远程服务器 IP 之前植入更多恶意有效负载。

4% 的恶意 DNS 请求都来自计算机犯罪或黑帽黑客网页，其中一些犯罪分子会试图使用网络浏览器散布关于欺诈的信息，或从事其他类型的在线犯罪活动。这一比例相对较低，可能是因为这些链接要么通过匿名化节点进行路由，要么被公司代理、防火墙检测并阻止，最后被关闭。

图 11：

十大被仿冒品牌

2019 年垃圾邮件中被仿冒的 10 大品牌细分，以百分比显示 10 大品牌（来源：IBM X-Force）



钓鱼攻击者仿冒技术公司、社交媒体

2019 年，钓鱼攻击仍是一个主要的威胁媒介，X-Force 数据显示，钓鱼攻击活动中最常见的伪冒品牌是科技和社交媒体平台。用户很难用肉眼分辨出伪冒域名，并且这些域名通常会模仿被仿冒公司使用的合法域名。一个真假难辨的网站如果与“真身”足够相似，就很容易让用户放松警惕，在恶意网站上泄露个人信息。

这一数据是通过分析 2019 年由 Quad9 拦截的所有恶意域名，并在 IBM X-Force 域名抢注检测的基础上获得的。

将社交媒体或内容流媒体网站（例如 Instagram 和 Spotify）作为目标，可能无法向威胁实施者提供易于获利的数据，例如窃取 Google 或 Amazon 帐户。但是威胁实施者可以寄希望于个人用户，希望他们在帐户与服务之间重复使用密码，并尝试使用收集的凭证访问同一用户持有的更有价值的帐户。

最常受到攻击的行业

在当今的威胁形势下，某些类型的攻击会因为威胁实施者的动机而具有特殊性，这意味着网络安全风险管理在不同行业间可能会有天壤之别。

为了全面了解每年最容易成为攻击目标的行业，X-Force 研究人员对我们监测到的各行业的攻击数量进行了排名。根据 X-Force 管理网络提供的攻击和安全事件数据，从事件响应服务中获得的数据和洞察以及公开披露的事件，确定了最常受到攻击的行业。

图 12：

十大目标行业

2019 年与 2018 年 10 大最常受到攻击的行业对比，按攻击数量计算（来源：IBM X-Force）

行业	2019 年排名	2018 年排名	变化情况
金融服务	1	1	–
零售	2	4	2
运输	3	2	-1
媒体	4	6	2
专业服务	5	3	-2
政府	6	7	1
教育	7	9	2
制造	8	5	-3
能源	9	10	1
医疗保健	10	8	-2

图 12 所示为 2019 年最常受到攻击行业及其相比 2018 年变化情况的对比图。

不难看出，金融服务行业排名靠前，零售行业也愈发受到攻击者的“青睐”。媒体和娱乐公司、教育以及政府机构同样也是如此。

下面的章节将根据各种数据源深入分析目标攻击的相对频率，以及我们在 2019 年针对每个行业的调查结果。有些行业的描述凸显了近年来格外活跃地攻击某一行业的威胁实施者，但此列表并不详尽，只包括 2019 年之前的数据。X-Force IRIS 跟踪并概述了数十个民族国家赞助的网络犯罪组织。未分类的活动和自然状态下发现的活动都在活动“HIVE”中进行跟踪。活动达到了严格的分析阈值之后，就会过渡到 IBM Threat Group (ITG)，其依据是一系列 TTP、基础架构、目标以及间谍情报技术。

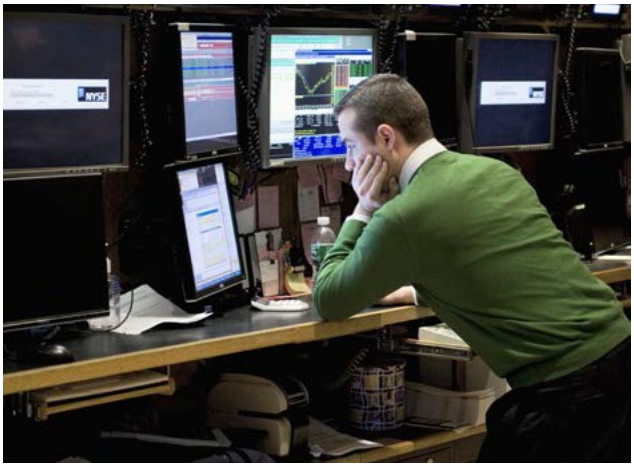
金融与保险

2019 年，金融保险行业连续第四年在最容易受到攻击的行业排行中榜上有名。在前 10 大目标行业中，对这一行业发起的攻击占到了所有攻击的 17%。

在经常针对金融实体发起攻击活动的网络威胁实施者中，利欲熏心的网络犯罪分子占有最大的比重，金融公司对网络犯罪分子的吸引力显而易见：可能迅速获得高额回报，一旦得手就能将数百万美元收入囊中。

X-Force 事件响应活动的数据显示，尽管公开披露的数据泄露较少，金融保险仍是最容易受到攻击的行业。

这表明，相对于其他行业而言，金融保险公司会遭遇更多攻击，但他们也会采取更有效的工具和流程，在攻击活动酿成重大事件之前发现并遏制威胁。金融公司也更愿意测试他们的响应计划，并且在使用 IBM Security Command Centers 来准备应对网络攻击的组织中，大部分都是金融公司。由 Ponemon Institute 执行并由 IBM Security 赞助的 2019 年数据泄露成本报告[4] 称，针对相关场景广泛测试事件响应计划和团队，可有效规避因为数据泄露造成的经济损失。举例来说，在网络范围内对其事件响应计划进行了广泛测试的组织遭到破坏，其平均损失要比 392 万美元的数据泄露总体平均成本少 32 万美元。



2019 年针对金融行业组织的主要威胁团体是 ITG03(Lazarus)、ITG14 (FIN7) 和不同的 Magecart 派系。TrickBot、Ursnif 和 URLZone 等银行木马是 2019 年令银行深受困扰的头号威胁，这些木马会接管并欺诈客户帐户。

4 由 Ponemon Institute 执行并由 IBM 赞助的年度数据泄露成本报告。

零售

2019 X-Force 数据显示，零售行业遭受的攻击在所有行业中排名第二。在前 10 大行业中，零售业所遭受的攻击占 16%，与 2018 年排名第四的 11% 相比有所上升。2019 年，零售业遭遇的网络攻击数量排名第二。

根据 X-Force IRIS 提供的数据和公开披露的数据泄露信息，零售行业在 2019 年排名第二。最常见的以零售行业作为攻击目标的威胁实施者是受经济利益驱动的网络犯罪分子，他们瞄准零售业，是为了窃取消费者的个人身份信息 (PII)、支付卡数据、金融数据、购物历史记录以及忠诚计划信息。犯罪分子经常利用这些数据接管客户帐户，欺骗客户并在各种身份窃取场景中重新利用该数据。

网络犯罪分子在 2019 年针对零售商的一种常用攻击伎俩是销售点 (POS) 恶意软件和电子商务支付卡窃听，每种攻击都在通过物理支付终端或在线交易时窃取支付卡信息。

尤为值得一提的是，一组归属于 Magecart 的网络犯罪派系一直将第三方支付平台和知名的在线零售商作为攻击目标，直接将恶意 JavaScript 代码注入其网站的卡支付页面。该代码在结帐过程中执行，会将受害者的支付卡信息传输给网络犯罪分子，此外，还可以获取目标供应商的信息。

X-Force IRIS 事件响应人员在 2019 年的多次泄露中监测到了此类攻击，同时表示，尽管恶意代码片段可能微不足道，但针对基础平台的后端破坏可能会牵一发而动全身，使得犯罪分子能够使用相同的技术攻击数千家商店。

攻击零售行业的主要威胁团伙包括：

ITG14 (FIN7)	Hive0061 (Magecart 10)
HIVE0065 (TA505)	Hive0062 (Magecart 11)
ITG08 (FIN6)	Hive0066 (Magecart 12)
Hive0038 (FIN6)	Hive0067 (FakeCDN)
Hive0040 (Cobalt Gang)	Hive0068 (GetBilling)
Hive0053 (Magecart 2)	Hive0069 (Illum Group)
Hive0054 (Magecart 3)	Hive0070 (PostEval)
Hive0055 (Magecart 4)	Hive0071 (PreMage)
Hive0056 (Magecart 5)	Hive0072 (Qoogle)
Hive0057 (Magecart 6)	Hive0073 (ReactGet)
Hive0058 (Magecart 7)	Hive0083 (Inter Skimmer)
Hive0059 (Magecart 8)	Hive0084 (MirrorThief)
Hive0060 (Magecart 9)	Hive0085 (TA561)

除了在线电子商务 Skimmer 恶意程序外，销售点恶意软件仍是网络犯罪分子在零售商实体店的惯用手段，伺机在交易过程中或在将数据写入内存时窃取销售点机器和后端服务器中的支付卡数据。

运输

运输行业是任何国家或地区的重要基础设施中必不可少的一部分。从事该行业的公司通过三种主要运输方式（包括陆运，海运和空运）提供工业和消费者服务，从而推动经济发展。运输行业是 2019 年第三大目标行业，攻击频率从 2018 年的 13% 下降至 2019 年的 10%。

运输行业紧随金融和零售行业之后排名第三，可以看出运输公司运营的数据和基础设施越来越有吸引力。无论是网络犯罪分子还是民族国家威胁实施者，同样也对这些资产虎视眈眈。运输公司拥有的信息成为了网络犯罪分子眼中诱人的“蛋糕”，这些信息包括个人身份信息、履历信息、护照号码、忠诚计划信息、支付卡数据和旅行路线等。

在运输行业，尤其是航空公司和机场，更是网络犯罪分子和民族国家对手日益青睐的目标，他们希望跟踪感兴趣的旅行者，或者在暗网上出售旅行者的个人信息，以此方式坐收渔利。

与其他行业相比，运输行业的网络威胁往往伴随着更高的风险，因为攻击可能会产生潜在的蝴蝶效应，让人们面临生命危险，并且有可能对依赖运输服务来开展运营的其他行业产生连锁影响。

2019 年对运输行业发起攻击的威胁实施者团伙有所不同，网络犯罪团体和民族国家对手都对全球的运输组织发起了攻击。

攻击运输行业的主要威胁团伙包括：

ITG07 (Chafer)	ITG17 (Muddywater)
ITG09 (APT40)	Hive0016 (APT33)
ITG11 (APT29)	Hive0044 (APT15)
ITG15 (Energetic Bear)	Hive0047 (Patchwork)

媒体与娱乐

根据 X-Force 的攻击目标排名，排名第四的是媒体行业，该行业受到的攻击在前十大行业的所有攻击中占 10%。媒体行业的占比与 2018 的 8% 相比有所上升，排名从第六位升至第四位。

媒体行业包括许多知名的子行业，例如电信公司，以及生产、处理和分发新闻媒体和娱乐的公司。对于试图影响公众舆论、控制信息流或保护其组织或国家声誉的网络攻击者来说，媒体和娱乐行业是一个高价值目标。具体来说，民族国家团队可以将负面的媒体内容视为对其国家安全的重大威胁，而网络罪犯则发现，对媒体和娱乐行业的攻击可以获取丰厚的回报，因为他们可以凭借窃取未播出的媒体内容勒索赎金。

2019年，机会主义网络犯罪分子和民族国家对手通常会将目标锁定在这一行业。

攻击媒体与娱乐行业的主要威胁团伙包括：

ITG03 (Lazarus)
Hive0003 (Newscaster)
Hive0047 (Patchwork)

专业服务

专业服务行业是指专门为其他行业提供专业咨询服务的公司，比如一些提供法律服务、咨询、HR 和专业客户支持的公司，都属于这一行业。X-Force 数据显示，专业服务行业遭受的攻击数量在 10 个行业所有攻击中的占比为10%，与 2018 年的 12% 相比略有下降。

公开披露的数据泄露信息表明，在排名的所有行业中，专业服务泄露的记录数量最多。这些公司当中有很多都会从客户那里获取高度敏感的数据，例如法律诉讼数据、用于会计和税务的数据，对于那些一心想要谋取钱财或内部信息的攻击者而言，这些都是充满诱惑力的目标。

此外，该行业还包括一些技术公司，他们因为拥有第三方访问权限而受到越来越多的关注，攻击者可以利用他们去破坏这些公司所服务的更大、更安全的组织。

此外，专业服务公司的日常工作流也便于犯罪分子通过钓鱼攻击电子邮件和恶意宏来创建攻击媒介。许多专业服务公司高度依赖生产力文件，例如 Word 和 Excel 文档附件来签订合同，与客户沟通以及完成日常工作任务。宏的使用是网络犯罪分子利用的最臭名昭著的攻击媒介之一，他们将恶意脚本植入此类文件中，任何组织都无法彻底拦截此类脚本。

2019 年对专业服务发动攻击的知名威胁实施者团伙：ITG01 (APT10, Stone Panda)，一个可能起源于中国的民族国家赞助团体。

政府

在我们的排名中，政府行业是第六大最常受到攻击的行业，其攻击数量在前 10 大行业中占 8%，这一比例与去年持平，但排名比 2018 年（第七名）略有上升。

政府部门是一个充满诱惑力的高价值目标，民族国家网络威胁实施者希望从中获得领先于对手的优势，黑客活动分子希望从中获得机密信息或者证明自己的技术实力，网络犯罪分子希望通过勒索或窃取数据谋取钱财。

近年来，市政府受到的攻击尤为猛烈，因为他们的安全性低于私有企业，网络犯罪分子看准了这一软肋，希望从中勒索钱财。在威胁实施者眼中，政府实体拥有大量宝贵资产，其中主要是机密信息和可能的国家机密，包括政府雇员和代理人的个人识别信息、财务信息、内部通信以及关键网络的功能。

民族国家威胁实施者向来对政府部门实体虎视眈眈，X-Force IRIS 评估称，他们最有能力发起攻击。但在 2019 年，网络犯罪组织也越来越多地将目标对准政府实体，试图加密和把持政府需要操作的赎金数据，在省市一级更是如此。

2019 年，仅在 1 月到 7 月之间，就有 70 多个政府实体受到勒索软件的攻击。网络犯罪分子还窃取了数据（包括来自国防网站的数据），然后将数据泄露到暗网上。臭名昭著的黑客分子发现政府是一个有吸引力的目标，尤其是当他们希望就有争议的问题发表声明时更是如此。与私营企业相比，政府组织的网络安全资金水平往往略逊一筹，但他们仍需要为选民提供一致的服务，这便进一步加剧了威胁实施者对这些组织的挑战。

2019 年，针对政府机构发起攻击的知名威胁实施者团伙：各种网络犯罪参与者和民族国家赞助的团体。

教育

教育行业受到的攻击数量在前 10 大行业中占 8%，与 2018 年的 6% 相比略有上升，成为排名第七的最常受到攻击的行业。

教育行业拥有大量宝贵资产，受经济利益驱动的威胁实施者和民族国家威胁实施者对这些资产觊觎已久。从知识产权 (IP) 到 PII，教育组织永远是各类威胁实施者眼中的一块肥肉。

敌对实施者各怀鬼胎，使用不同的初始入侵媒介破坏学术机构网络，但我们的监测结果显示，最常见的方法仍是钓鱼攻击电子邮件，且通常会是针对特定的学术机构或研究领域量身定制的钓鱼攻击电子邮件。

教育行业组织通常有着庞大而多样化的 IT 基础架构和数字足迹。他们掌控着不同的资产，为数量不断攀升的用户提供服务，其中有职员、学生，也有承包商。攻击面如此广泛，要保障其安全更是难上加难，威胁实施者便趁机开展各种恶意活动。2019 年 10 月份发布的报告显示，单单在美国，2019 年就至少有 500 所学校遭受了网络攻击，其中大多数都是勒索软件发起的攻击。

教育行业一些值得关注的更复杂的攻击包括：民族国家威胁实施者入侵大学网络，然后将它们作为集结地，大肆感染媒体组织和军事承包商。同样，以美国资助的研究作为攻击目标的攻击者，也会绞尽脑汁入侵大学网络，伺机窃取一些价值连城的知识产权。

攻击教育行业的主要威胁团伙包括：

ITG05 (APT28)
ITG12 (Turla Group)
ITG13 (APT34)
ITG15 (Energetic Bear)
ITG17 (Muddywater)
Hive0075 (DarkHydrus)

IBM X-Force IRIS 公布了一项有高度把握的评估结果，宣称受经济利益驱动的威胁实施者和隶属于政府部门的威胁实施者为了获取重要信息，会继续将此行业作为攻击目标。

2019 年此行业的知名威胁实施者团伙包括：投机取巧的网络犯罪势力和来自中国、俄罗斯和伊朗的民族国家对手。

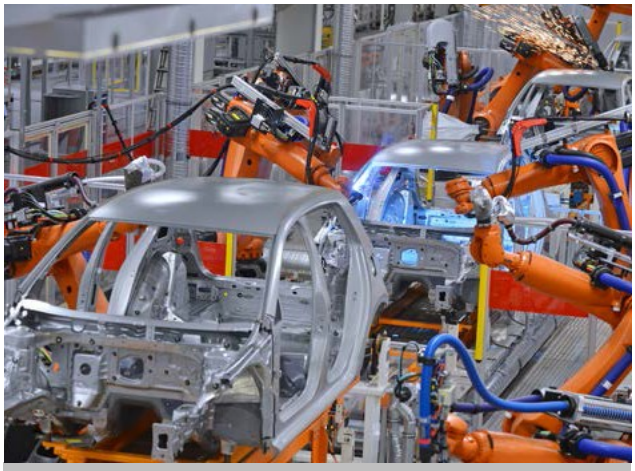
制造

制造商通过金属、化工、生产资料和电子产品推动经济发展，但也不能免于各种 IT/OT 威胁。在前 10 大最常受到攻击的行业中，制造业所遭受的攻击数量占 8%，排名第八，与 2018 年的 10% 相比有所下降。

制造业所遭受的攻击数量比上一年要少，数字的下降反映出一个事实，即：在很多情况下，制造行业的数据泄露都未涉及到必须合法披露且受到法规监管的信息。因此，有些攻击并未公开披露，这样一来，尽管制造商受到了攻击，但披露的数量却少于实际数量。

制造商也会运营 IT 和 OT 环境，因此也同样面临着影响 ICS 和 SCADA 系统的威胁。不过，尽管该行业的信息安全在过去一直落后，但挪威制造商对 2019 年一次成功的重大勒索软件攻击的公开回应，却可能表明该行业正在改变其网络安全方法。

寻求经济利益和知识产权的网络犯罪分子或民族国家威胁实施者可能对制造行业的公司构成最大的网络威胁。2019 年针对制造商的最常见攻击手段之一是商务电子邮件入侵 (BEC) 欺诈，如果他们经常与外国供应商开展业务，则更是雪上加霜。在这种情况下，攻击者会破坏公司的电子邮件服务器，甚至是电子邮件帐户，攻击者会将自己插入现有的通信线程中，最终将数百万美元转移到他们控制的帐户中。



针对制造行业发起攻击的知名威胁团伙包括：

ITG01 (APT10)
ITG09 (APT40)
HIVE0006 (APT27)
Hive0013 (OceanLotus)
Hive0044 (APT15)
Hive0076 (Tick)

此外，制造商还容易受到供应链攻击，民族国家对手可能会利用供应链在他们制造的产品中植入后门或恶意软件，然后再将其运送到其他国家或地区。

在财务动机方面，攻击者可能将制造商作为获取商业秘密和知识产权的目标。组织花费数年时间开发的研究可以迅速为暗网中的网络罪犯带来利润，或者提升一个国家的经济或国防优势 - 对国防和军事设备制造商而言更是如此。

X-Force 数据显示，勒索软件、钓鱼攻击和 SQLi 注入攻击也会经常攻击制造行业。

能源

2019 年，能源行业是第九大最常受到攻击的行业，它所遭受的攻击数量在 10 大行业的总攻击和事件数量中占 6%。这一行业排名与 2018 年持平，2018 年遭受的攻击数量也占总数量的 6%。

能源行业的公司备受网络公司的青睐，部分原因在于，这些公司重要性高，堪称各国重要基础设施的支柱。各种形式的能源对经济、国家安全以及城市和行业的日常运转有着举足轻重的作用。

对能源行业发动攻击的目标可能各不相同。能源公司一些利润丰厚的资产，例如客户数据、财务资料、商业机密和专利技术信息等，其价值与其他行业公司的资产不相上下。

真正让能源行业与众不同的是，ICS 系统和管理它们的 SCADA 系统可能受到物理破坏。对于希望监视或控制目标设施操作的对手而言，这些系统是非常有价值的目标；举例来说，当涉及到网络战，而且关系到竞争对手国家的核设施时，尤其如此。该行业还会受到破坏性恶意软件（例如 ZeroCleare）的攻击。

以中断 ICS 系统运行为目的而发起的攻击一旦成功，就可能对依赖能源行业提供的电力、天然气、石油或其他资源的客户造成毁灭性影响。在曾经针对乌克兰发电厂发起的一系列事件中，都可以看到此类攻击以及由此产生的严重后果，据称这些袭击是由俄罗斯发起，目的是要进行物理破坏。

攻击能源行业的主要威胁团伙包括：

ITG01 (APT10)	HIVE0006 (APT27)
ITG09 (APT40)	Hive0016 (APT33)
ITG07 (Chafer)	Hive0044 (APT15)
ITG11 (APT29)	Hive0045 (Goblin Panda)
ITG12 (Turla Group)	Hive0047 (Patchwork)
ITG13 (APT34)	Hive0076 (Tick)
ITG15 (Energetic Bear)	Hive0078 (Sea Turtle)
ITG17 (Muddywater)	Hive0081 (APT34)
Hive003 (APT35)	

医疗保健

医疗保健行业是第十大目标行业，所遭受的攻击占 10 大行业所有攻击数量的 3%，与 2018 年的排名第八和 6% 的攻击相比略有下滑。

大量证据表明，利欲熏心的网络犯罪分子是医疗保健行业网络和医疗设备的主要攻击者，他们的目的是窃取病历，然后在暗网上出售，或者是加密网络连接的设备，以干扰活动并挟持公司以勒索资金 。

医院和疗养院网络中断会迫使医疗机构支付勒索软件攻击费用，以尽快恢复网络运营并保障患者生命安全。有时候赎金会高到离谱，例如 2019 年攻击者发起 Ryuk 攻击之后索要了 1400 万美元的高额赎金。

2020 年，医疗保健行业会继续改进其安全措施以增强数据保护。鉴于勒索软件攻击频繁发生，医院必须增强事件响应能力，并防范针对一些不安全的医疗设备发起的新攻击，这些攻击很容易让医院束手就擒并被心怀不轨的攻击者所左右。

对本行业发起攻击的知名威胁团伙包括一些受经济利益驱动的网络犯罪团伙，例如操作 Ryuk 勒索软件的团伙。尽管勒索软件攻击的确凸显了当医院受到感染时可能发生的危机，但民族国家威胁实施者对此领域的兴趣并不持久。

全球中心洞察

2019 年，威胁实施者的攻击目标遍布所有地区，且北美、亚洲和欧洲的活动最为频繁。

X-Force 研究人员还发现，在 2019 年针对中东和南美的威胁实施者活动中，前者遭受的黑客活动分子和民族国家攻击更多，而南美则主要受到追逐经济利益的威胁实施者的攻击。

在本节中，我们将更深入地研究发生在这些地域的攻击，以更好地了解 X-Force 所监测到的攻击的特性，侧重于各个领域的主要威胁实施者以及 2020 年要留意的重要日期，提防可能会增加的威胁实施者活动。对于一些地区，我们突出显示了近年来在该地区格外活跃的威胁实施者，但该列表并不详尽，只列出了 2019 年之前的数据。本节使用了如上所述的 IBM Threat Group 命名方法，还利用了 IBM 全球事件响应中的数据以及公开披露的泄露数据。

北美

北美在威胁实施者攻击的所有类别中排名最高，占 2019 年所有事件中的 44%。

北美有很多潜在目标，还拥有大量互联网基础架构，是令犯罪实施者垂涎的攻击目标。2019 年，北美泄露的记录超过 50 亿条。

2019 年，IBM 对多起北美事件做出了回应，发现这些事件都使用了商品化的恶意软件 - 可以在地下市场上购买或免费获得的代码。商品恶意软件可能很难识别，却能快准狠地达成犯罪目标。

2019 年，向北美发起的民族国家威胁实施者活动保持不变，但未监测到重大事件。近来美中之间的贸易谈判可能会增加对在中美两国开展业务的组织的攻击，只要谈判尚无结果，这些组织就应保持警惕。

即将举行的具有重大网络安全历史意义的活动：

7 月 13 日
（美国民主党全国代表大会）
8 月 24 日
（美国共和党全国代表大会）
11 月 3 日
（美国总统选举）

对此地区发起攻击的威胁实施者团伙包括：

ITG05 (APT28)
ITG08 (FIN6)
ITG11 (APT29)
ITG15 (Energetic Bear)
Hive0082 (Cobalt Dickens)
Hive0042 (Kovter)
Hive0016 (APT33)
Hive0006 (APT27)
Hive0003 (APT35)
ITG01 (APT10)
ITG03 (Lazarus)
ITG04 (APT19)
ITG09 (APT40)
ITG07 (Chafer)

2019 年 X-Force 事件响应活动中监测到的最突出的攻击活动：

商务电子邮件入侵、勒索软件、以金融行业为目标的民族国家攻击活动。

亚洲

X-Force 分析结果显示，亚洲获得了第二高的风险评级，在公共泄露事件中排名第二，事件数量占 2019 年总数量的 22%。2019 年，亚洲泄露的记录超过 20 亿条，仅次于北美。

有大量威胁实施者都以亚洲的组织作为攻击目标，其中以朝鲜半岛、日本和中国尤为突出。在亚洲监测到的许多攻击都采用了民族国家威胁实施者 TTP。ITG10 便是其中之一，可能是对韩国实体发起攻击的朝鲜威胁实施者。另一个便是 ITG01，可能是针对日本发起攻击的中国威胁实施者。

近期在亚洲发生的地缘政治事件增加了在该地区民族国家发起活动的可能性。中国香港爆发的民主抗议和随后的镇压让中国陷入不安之中。朝鲜与其邻国间剑拔弩张的局面让这些活动更加猖獗。印度对克什米尔地区的蚕食同样导致该地区紧张局势加剧。

进入 2020 年，对这些潜在的不稳定地缘政治风险的监测对于了解在该地区运营的组织所面临的风险至关重要。

即将举行的具有重大网络安全历史意义的活动：

7 月 24 日
（2020 年东京奥运会）

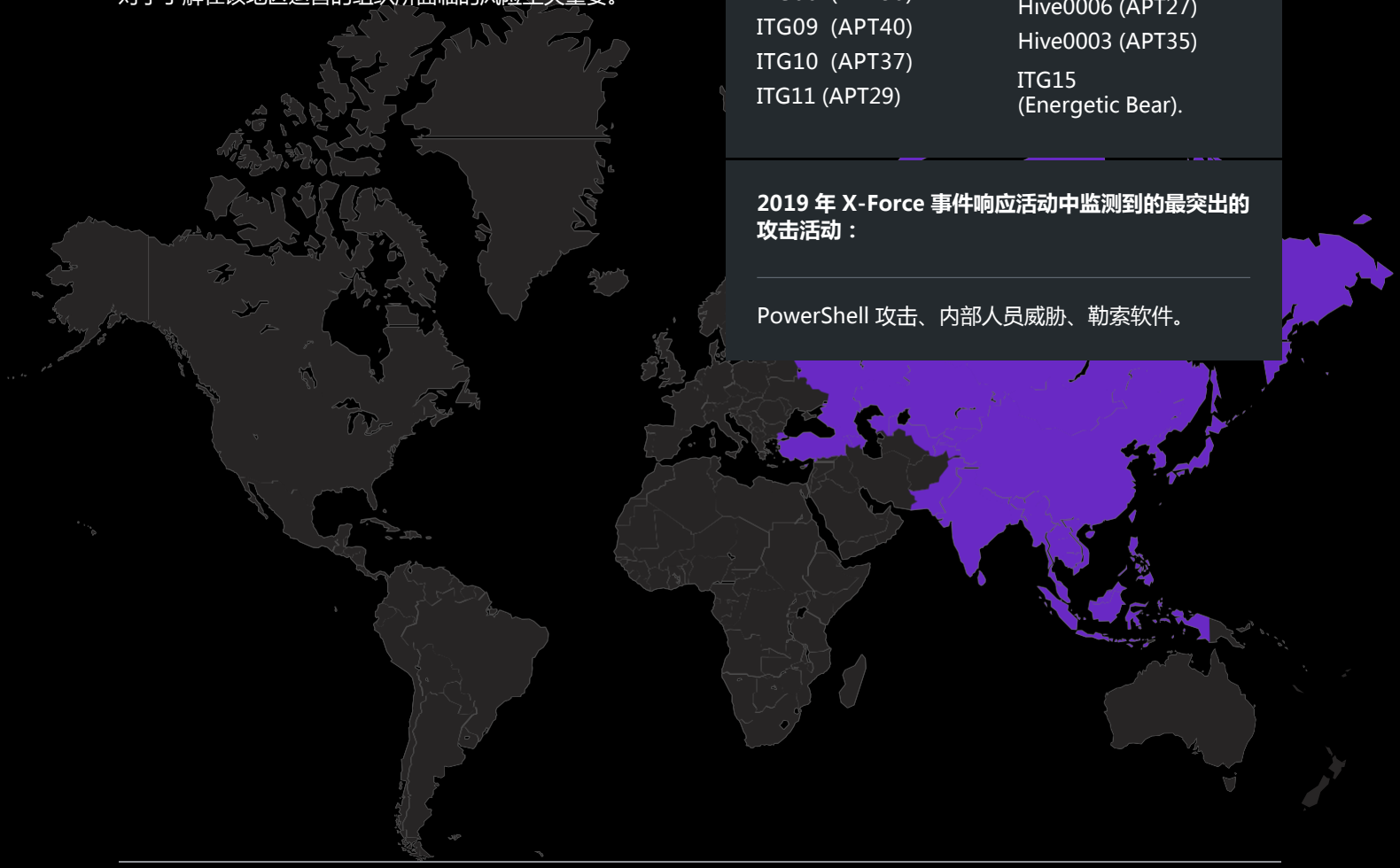
10 月 10 日
（中国台湾独立日）

对此地区发起攻击的威胁实施者团伙包括：

Hive0013 (OceanLotus)
Hive0044 (APT15)
Hive0045 (Goblin Panda)
Hive0049 (Samurai Panda)
ITG01 (APT10)
ITG03 (Lazarus)
ITG05 (APT28)
ITG06 (APT30)
ITG09 (APT40)
ITG10 (APT37)
ITG11 (APT29)
ITG16 (Kimsuky)
Hive0016 (APT33)
Hive0040 (Cobalt Gang)
Hive0047 (Patchwork)
Hive0063 (DNSpionage)
Hive0076 (Tick)
Hive0079 (Labryinth Cholima)
Hive0006 (APT27)
Hive0003 (APT35)
ITG15 (Energetic Bear).

2019 年 X-Force 事件响应活动中监测到的最突出的攻击活动：

PowerShell 攻击、内部人员威胁、勒索软件。



欧洲

欧洲沦为与亚洲相似的恶意活动受害者，事件数量占总数量的 21%。

亚洲受到的攻击大多来自对手国，欧洲则不同，它们受到的攻击主要来自受经济利益驱动的威胁实施者。之所以存在这种差异，可能是因为根据货币汇率，从欧洲公司窃取信息的可能性更大。另外，其犯罪动机可能是为了窃取知识产权，然后将其出售给竞争对手以获取巨额利润。

进入 2020 年，英国脱离欧盟（脱欧）可能会在黑客活动分子圈内产生连锁反应，但 2019 年并未监测到攻击活动。此外，主要欧盟国家（德国、法国）即将到来的大选活动，也可能成为希望利用政治在这些国家兴风作浪的民族国家威胁实施者的目标。

即将举行的具有重大网络安全历史意义的活动：

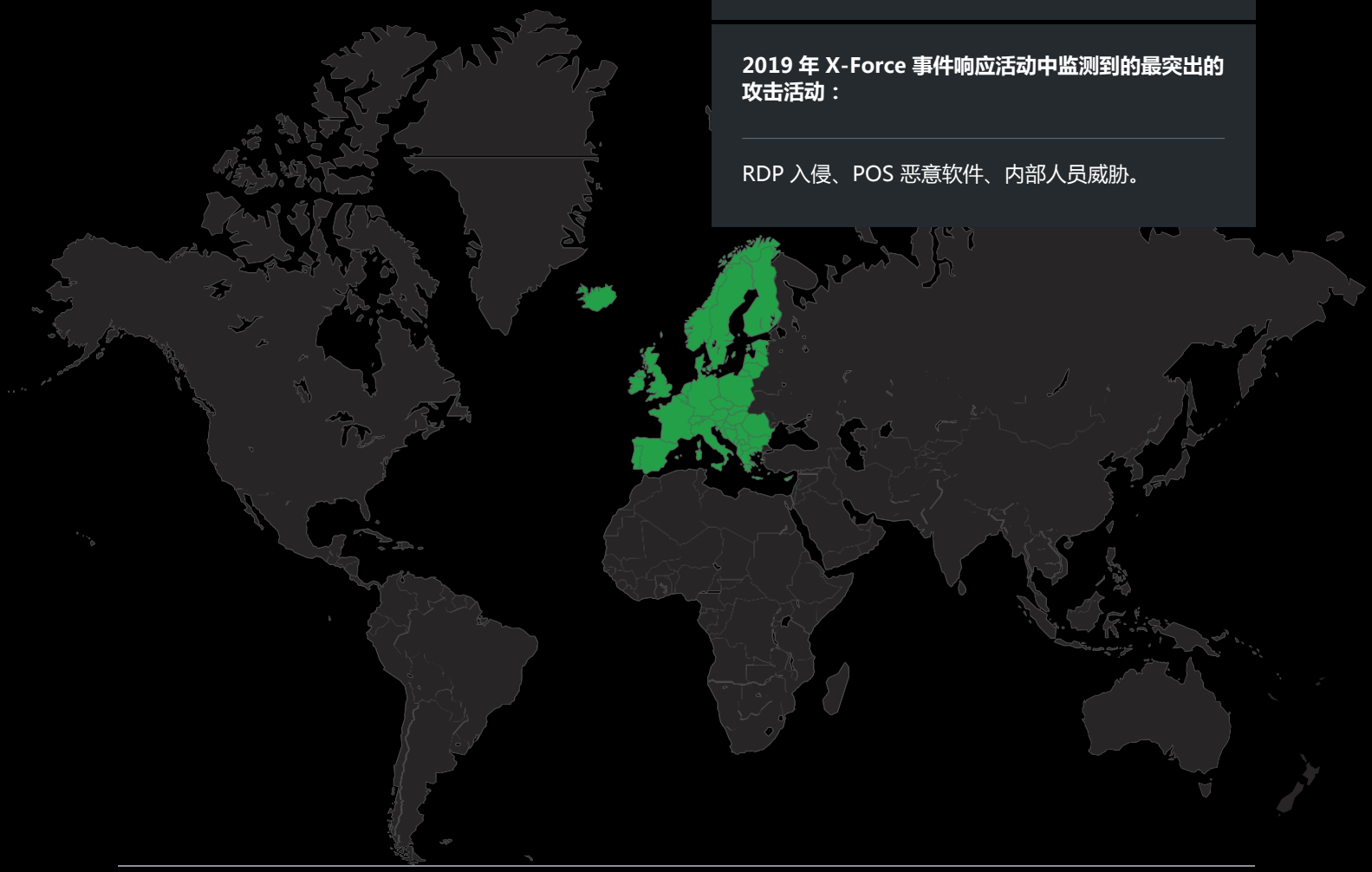
1 月 31 日
（英国根据第 50 条规定退出欧盟）
6 月 28 日
（乌克兰宪法日/NotPetya 纪念日）

对此地区发起攻击的威胁实施者团伙包括：

ITG05 (APT28)
ITG08 (FIN6)
ITG12 (Turla)
ITG15 (Energetic Bear)
ITG09 (APT40)
ITG07 (Chafer)
ITG11 (APT29)
ITG14 (FIN7)
ITG17 (Muddywater)
Hive0006 (APT27)
Hive0003 (APT35)
Hive0013 (OceanLotus)
Hive0044 (APT15)
Hive0063 (DNSpionage)

2019 年 X-Force 事件响应活动中监测到的最突出的攻击活动：

RDP 入侵、POS 恶意软件、内部人员威胁。



中东

2019 年，X-Force IRIS 监测到了大量与民族国家关联的事件，给中东的许多组织带来了影响，但 2019 年威胁实施者活动的总体指标仍相对较低，该地区的事件占 7%。

活动减少的原因有很多，例如其他地区可以为网络犯罪活动带来更高的投资回报等。但是，与其他地区的不同之处在于，与世界其他地区相比，中东的黑客活跃分子和民族国家活动比例较高。

2019 年，黑客分子活动引发了政治动乱，发生了多起涉及伊朗的重大事件。同样，民族国家活动，例如打着追求伊朗国家利益旗号的 ITG13，通过在该地区发动破坏性攻击，对从事能源行业的组织发起攻击。

也门的政治动荡和持续武装冲突继续带来网络威胁活动的风险，冲突各方都在利用网络攻击来传播其信息并创造收入。这些风险很可能会持续到 2020 年，因为各方在这场持续不断的冲突中仍在不断地公开威胁对方。

即将举行的具有重大网络安全历史意义的活动：

11 月 21 日
（2022 俱乐部世界杯足球赛，卡塔尔）

对此地区发起攻击的威胁实施者团伙包括：

Hive0044
ITG07 (Chafer)
ITG13
Hive0081 (APT34)
Hive0078 (Sea Turtle)
Hive0075 (DarkHydrus)
Hive0063 (DNSpionage)
Hive0047 (Patchwork)
Hive0022 (Gaza Cybergang)
Hive0016 (APT33)
Hive0006 (APT27)
Hive0003 (APT35)
ITG17 (Muddywater)
ITG12 (Turla)
ITG11 (APT29)
ITG10 (APT37)
ITG09 (APT40)
ITG05 (APT28)
ITG01 (APT10)

2019 年 X-Force 事件响应活动中监测到的最突出的攻击活动：

破坏性恶意软件、DDOS 攻击、Web 脚本攻击。

南美

2019 年，南美洲也与严重的网络犯罪活动展开了殊死较量，但它并未获得与另外三个重点地区相同的关注度，事件数量仅占总数量的 5%。然而，该地区的活动仍在逐年增加，X-Force 监测到重大事件响应活动有所增加，在零售和金融服务行业尤为突出。

此地区监测到的事件中有勒索软件活动，该活动在 2019 年一直处于增长状态。

即将举行的具有重大网络安全历史意义的活动：

6 月 12 日
（2020 年美洲杯足球赛，哥伦比亚和阿根廷）

对此地区发起攻击的威胁实施者团伙包括：

Hive0081 (APT34)
Hive0044 (APT15
Hive0016 (APT33)
Hive0013 (OceanLotus)
Hive0003 (APT35)
ITG17 (Muddywater)
ITG12 (Turla)
ITG11 (APT29)
ITG05 (APT28)
ITG03 (Lazarus)
ITG01 (APT10)

2019 年 X-Force 事件响应活动中监测到的最突出的攻击活动：

商务电子邮件入侵、勒索软件、以金融行业为目标的民族国家攻击活动。

为 2020 年的弹性应对做好准备

根据 IBM X-Force 在此报告中揭示的重要发现，无论从事哪种行业，也无论在哪个国家或地区经营业务，只有充分了解最新威胁情报并培养强大的响应能力，才能在不断变化的威胁格局中规避威胁。

我们的团队为每个组织推荐了一系列举措，使其能够在 2020 年更好地应对网络威胁：

- 利用威胁情报，以更好地了解威胁实施者的动机和策略，从而对安全资源进行优先级排序。

- 在您的组织内组建事件响应团队并开展培训活动。如果不能组建团队，就掌握一种有效的事件响应能力，以确保及时响应有重大影响的事件。2019 年，IBM Security 监测到，及时遏制影响可显著削减相关成本，因为我们的团队及时干预 MegaCortex 感染活动，中途阻断了勒索软件攻击，从而避免了数千美元的损失。

- 对您组织的事件响应计划开展压力测试，以形成肌肉记忆。桌面演习或网络突击体验可以为您的团队提供重要的经验，从而有助于缩短响应时间，减少停机时间，最后做到即便发生泄露也能降低损失。

-

- 实施多因素身份验证（MFA）仍然是组织最有效的安全优先事项之一。2019 年，凭证盗窃或重复使用是威胁实施者最常用的攻击手段之一，MFA 可以有效地防患于未然，掐断攻击的苗头。

- 因为普遍利用钓鱼作为攻击媒介，请确保组织制定适当的解决方案来检测和拦截欺骗性域名，例如 Quad9。

- 及时备份，测试并离线存储备份。不仅要将备份落到实处，还要通过真实的测试来验证备份的有效性，这对确保组织的安全性至关重要。

未来展望及关键要点

2020 年，组织需要密切关注新威胁，同时也要警惕一些旧威胁。

- 2020 年，风险面会继续增长，目前已有超过 15 万个漏洞，还会有新漏洞被不断发现。
- 2019 年泄露的记录数量是 2018 年的四倍，2020 年仍会有大量记录因为泄露和攻击而丢失。
- 随着物联网设备，运营技术（OT）以及互联的工业和医疗系统越来越多，威胁实施者会继续物色不同的攻击媒介。
- 威胁实施者对恶意软件的使用会继续波动，2019 年，勒索软件、加密货币挖矿软件以及僵尸网络都曾“风光无限”。我们预计 2020 年会继续保持这种趋势，这就意味着，组织需要让自己远离各种随着时间不断变化的威胁。
- 勒索软件和加密货币挖矿软件的高级别代码创新，意味着这些威胁在 2020 年会不断演变，组织需要具备更好的检测和遏制能力。
- 垃圾邮件活动会继续肆虐，需要组织更加勤奋地制定黑名单，修补漏洞并监控威胁。
- 行业特定目标的逐年变化凸显了所有行业的风险，也更需要更先进、更成熟的网络安全计划。
- 组织可以利用其地理位置来确定最有可能的攻击者和攻击动机，以预估并减轻他们可能面临的一些相关风险。

关于 X-Force

IBM X-Force 致力于研究和监测最新的威胁趋势，向客户和公众普及新兴威胁及关键威胁方面的知识，同时交付安全内容，帮助 IBM 客户实现安全防护。

从基础架构、数据和应用保护到云及托管安全服务，IBM Seurity Services 拥有丰富的专业知识，可帮助您保护关键资产。IBM Security 目前正在为一些全球最先进的网络保驾护航，并聘请了大量的优秀人才为其服务。

了解有关 IBM Security 的更多信息 →

致谢

Michelle Alvarez
Dave Bales
Joshua Chung
Scott Craig
Kristin Dahl
Charles DeBeck
Ari Eitan (Intezer)
Brady Faby (Intezer)
Rob Gates
Dirk Harz
Limor Kessem
Chenta Lee
Dave McMillen
Scott Moore
Georgia Prassinos
Camille Singleton
Mark Usher
Ashkan Vila
Hussain Virani
Claire Zaboeva
John Zorabedian

IBM Security
New Orchard Rd Armonk, NY 10504

美国印刷
2020 年 2 月

IBM **Security**