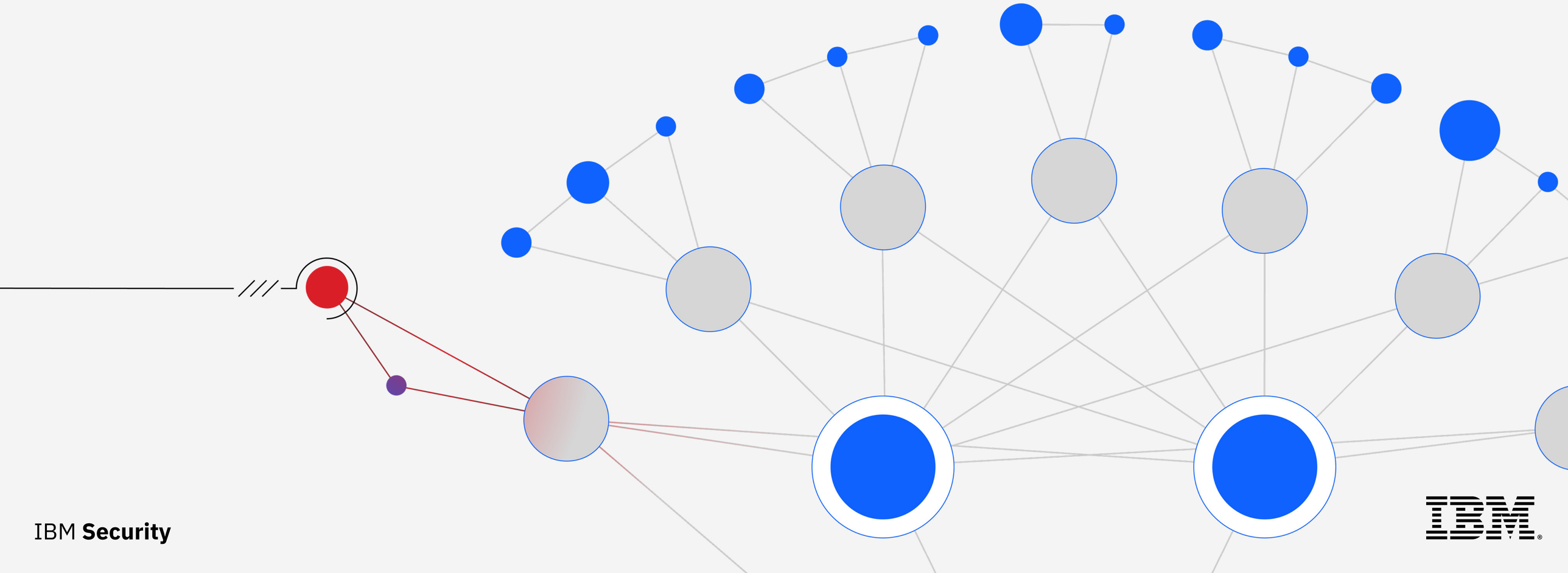
# 2023 年 X-Force 威胁情报指数

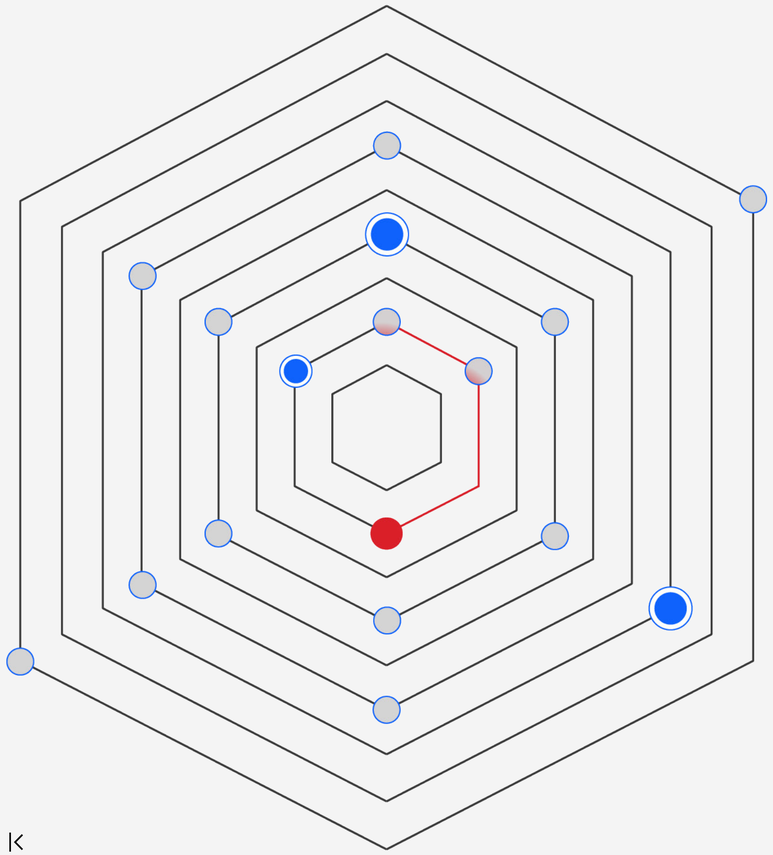


IBM **Security**

# 目录

01

# 执行摘要



2022 年又是一个网络安全动荡之年，混乱事件层出不穷，其中最突出的无疑是新冠疫情的持续影响和乌克兰军事冲突的爆发。2022 年充满动荡，全球经济、地缘政治和人类健康都面临严峻的挑战。而网络犯罪趁机蔓延发展，更加猖獗，我们为此付出了巨大的代价。

网络犯罪泛滥成灾。

IBM Security® X-Force® 发现，威胁参与者伺机而动，利用混乱无序的形势渗入全球各地的政府和组织。

2023 年 IBM Security X-Force 威胁情报指数跟踪全新和现有趋势与攻击模式，包含数十亿涉及网络和端点设备、事件响应 (IR) 参与、漏洞和数据库漏洞利用等的数据点。本报告包含我们从 2022 年 1 月到 12 月的全部研究数据。

我们将这些发现成果作为资源，提供给 IBM 客户、网络安全研究人员、政策制定者、媒体，以及广泛的安全行业专业人员和行业领导者社区。当前动荡不安的形势伴随着日趋复杂和恶意的威胁攻击，需要我们齐心协力为商业和民众提供网络安全保障。您比以往任何时候都需要威胁情报和安全洞察，以抢在攻击者前面，加强对关键资产的保护。

这样，您的企业依然可以蓬勃发展。

## 我们的数据分析在 2022 年的改变

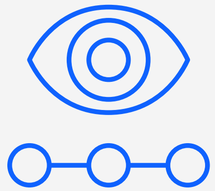
2022 年，我们修改了部分数据的检查方式。此变化使我们能够提供更具洞察力的分析，并更好地遵循行业标准框架。这反过来也可让您做出更明智的安全决策，更好地保护企业不受威胁侵害。

我们 2022 年的分析变化包括：

- **初始访问媒介：**采用 MITRE ATT&CK 框架跟踪初始访问媒介，可确保我们的研究发现与广泛的网络安全行业更匹配，帮助我们识别技术层面的重要趋势。
- **漏洞利用和零日漏洞入侵：**根据我们强大的漏洞数据库（包含差不多 30 年的数据）进行推演有助于为我们的分析提供背景，并识别漏洞带来的实际威胁。此流程还能为日渐下降的可武器化漏洞利用占比和有效的零日漏洞提供背景支持。
- **威胁参与者方法及其影响：**将威胁参与者在攻击中采取的行动步骤与该攻击事件的实际影响分开，便于我们识别事件的关键阶段。此流程反过来又揭示了响应者应在哪些方面做好准备，以应对事件后果。

02

# 报告要点



**针对所观察到的目标而采取的主要行动：**在 2022 年所有完成修复的事件中，近四分之一 (21%) 的各类后门攻击部署都属于针对目标所采取的主要行动。特别是年初多目标恶意软件 Emotet 的爆发，与去年同期相比，显著造成所观察到的后门活动增幅大幅跳升。虽然后门活动激增，但勒索软件至少从 2020 年以来就一直就是头号网络攻击手段，在 2022 年依然占有很大的比例，达到 17%，进一步加强了此恶意软件所造成的的持久威胁。

**勒索是对组织最常见的攻击影响：**勒索是威胁参与者选择造成的明显影响，占比达 27%。制造业受害者占勒索事件的 30%，承受着巨大的压力，而网络犯罪利用此行业牟利的趋势仍然在继续发展。

**网络钓鱼是首要的初始访问媒介：**网络钓鱼依然是主要的感染媒介，事件占比达 41%，然后是利用公众应用中出现的漏洞，占比 26%。由于 Microsoft 决定默认阻止宏，因此恶意宏感染不再是主要的初始访问媒介。恶意 ISO 和 LNK 文件使用在 2022 年升级为通过垃圾邮件传送恶意软件的主要策略。

**黑客行为和破坏性恶意软件增加：**俄乌战争打开了一扇门，展示了网络可如何推动现代战争，正如网络安全社区中的许多人所预计那样发展。虽然截至本文发表之时，最可怕的网络空间预测仍未发生，但是黑客行为和破坏性恶意软件明显增加了。X-Force 还观察到空前的网络犯罪世界变动——网络犯罪集团与 Trickbot 帮派之间的合作增加，均以乌克兰的组织为目标。

03

# 关键统计数据

## 27%

### 勒索攻击占比

在 X-Force 2022 年响应过的所有事件中，逾四分之一是威胁参与者企图向受害者敲诈金钱。他们使用的策略在过去十年间已发生改变，而随着威胁参与者日益猖獗地寻求牟利，该趋势预计将会持续下去。

## 21%

### 观察到所部署的后门攻击的事件占比

后门攻击部署是去年针对目标所采取的主要攻击行动，在全球报告的事件中超过五分之一。防御者的成功干预很可能阻止了威胁参与者实现更多目标，例如勒索软件攻击。

## 17%

### 勒索软件的攻击占比

而对一些攻击数量高企的勒索软件集团来说，即使在这混乱不堪的一年，勒索软件依然仅次于后门攻击部署，名列针对目标所采取的第二大攻击行动，继续对组织运营造成严重破坏。勒索软件的事件占比从 2021 年的 21% 降到了 2022 年的 17%。

41%

**初始访问网络钓鱼攻击的事件占比**
网络钓鱼攻击在 2022 年依然是首要入侵途径，使用此技巧获取初始访问的攻击在 X-Force 补救过的事件中占比高达 41%。

100%

**每月线程劫持攻击数增加**
与 2021 年的数据相比，2022 年每月线程劫持攻击数已增至之前的两倍。可导致 Emotet、Qakbot 和 IcedID 感染的垃圾电子邮件都大量使用了线程劫持手段。

52%

**报告的网络钓鱼套件企图获取信用卡数据的占比下降**
数据中分析的几乎每一个网络钓鱼套件都企图获取姓名 (98%) 和电子邮件地址 (73%)，然后是家庭住址 (66%) 和密码 (58%)。信用卡信息作为目标 在 2021 年的占比为 61%，但 2022 年不再是威胁参与者的主要目标——数据显示，2022 年网络钓鱼套件企图获取信用卡信息的占比仅为 29%，同比下降了 52%。

62%

**使用鱼叉式网络钓鱼附件进行网络钓鱼攻击占比**
攻击者更喜欢使用武器化附件，无论是单独部署，还是 与链接或服务伪装鱼叉式网络钓鱼一起部署。

26%

**2022 年已知漏洞利用占比**
2022 年已知漏洞利用占比为 26%。根据 X-Force 自 20 世纪 90 年代早期以来跟踪的数据显示，该比例近年一直在下降，表明妥善维护的补丁管理流程取得了不错的效益。

31%

**以亚太地区为目标的全球攻击占比**
亚太地区在 2022 年仍然是首要的攻击目标，威胁事件占比高达 31%。与 X-Force 2021 年在该地区响应过的事件相比，此统计显示攻击占比上升了 5%。

04

# 主要初始访问媒介

2022 年，X-Force 从跟踪初始访问媒介这个广泛类别（例如网络钓鱼和被盗凭证）转向至 MITRE ATT&CK Matrix for Enterprise 框架中列出的初始访问技能。该转变可让 X-Force 更精确地跟踪技巧层面的重要趋势，提供更多可即时使用和可交叉比较的数据，并且与广泛的行业标准化工作保持 一致。

**2022 年主要初始访问媒介**

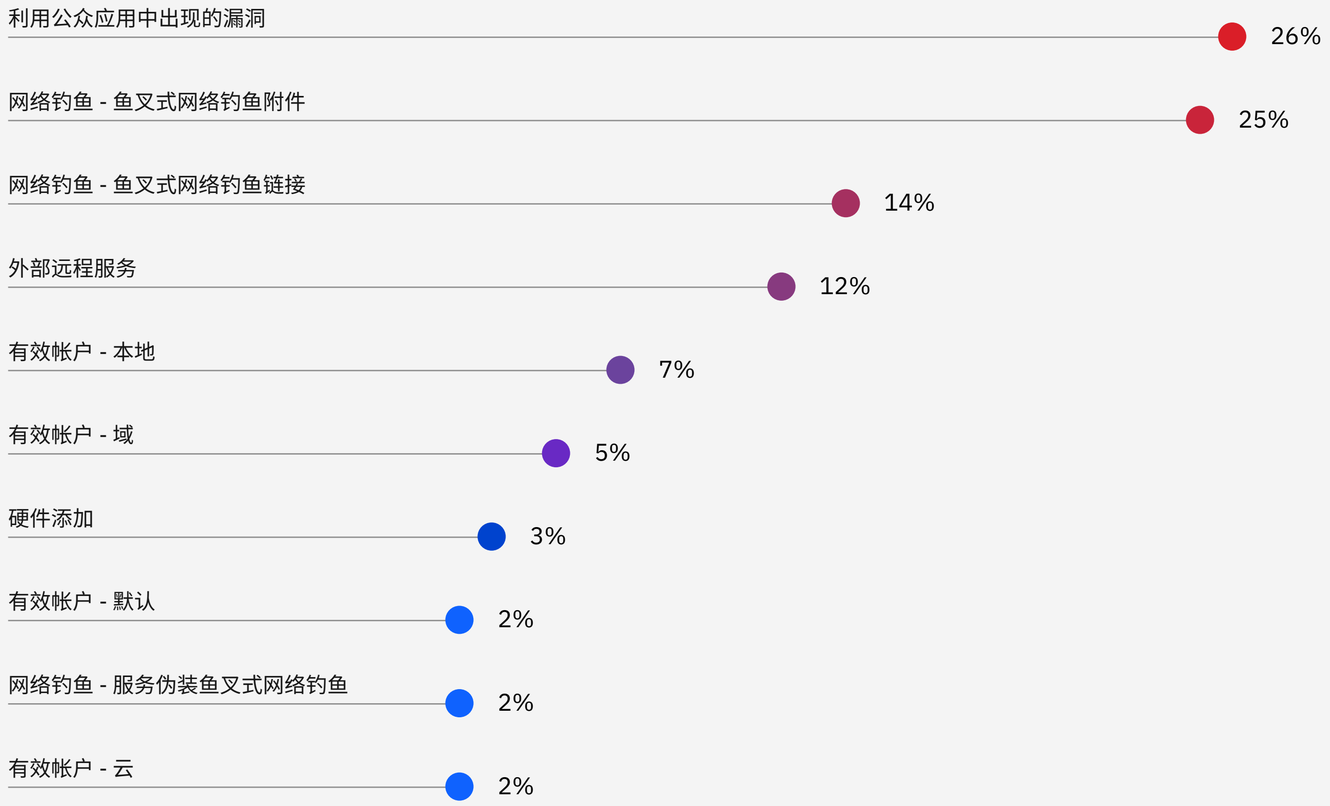



**图 1：**X-Force 2022 年所观察到的主要初始访问媒介。资料来源：X-Force

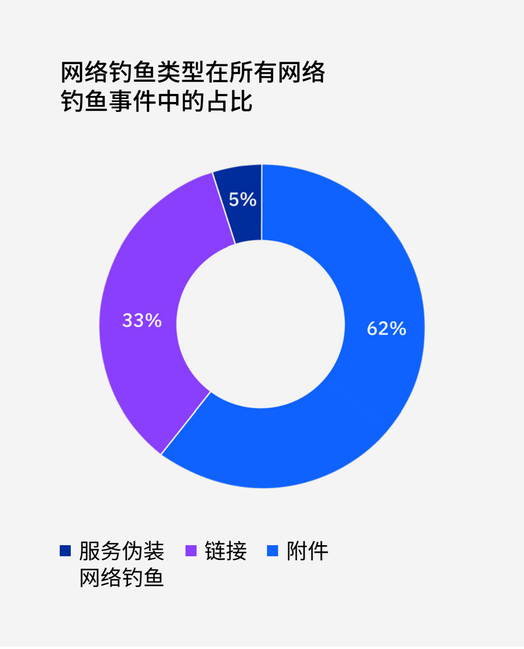



图 2：其他类型的网络钓鱼技巧在 X-Force 2022 年观察到的所有网络钓鱼事件中的占比。资料来源：X-Force

## 网络钓鱼

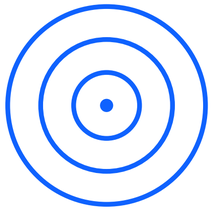
网络钓鱼 (T1566)（无论是通过附件、链接还是服务）依然是最主要的感染媒介，在 X-Force 2022 年补救过的所有事件中占比高达 41%。该占比在 2020 年为 33%，2021 年和 2022 年上升到 41%。在所有网络钓鱼事件中，62% 使用鱼叉式网络钓鱼附件 (T1566.001)，33% 使用鱼叉式网络钓鱼链接 (T1566.002)，5% 使用服务伪装鱼叉式网络钓鱼 (T1566.003)。X-Force 还发现，威胁参与者有时使用附件和服务伪装网络钓鱼或链接进行攻击。

2022 年的 IBM X-Force Red 数据进一步凸显网络钓鱼和凭证操作不当对威胁参与者的价值。在 2022 年对客户的渗透测试中，X-Force Red 发现，大约 54% 的测试显示存在对凭证的不当认证或处理。X-Force Red 对手模拟团队定期利用针对多重身份验证 (MFA) 令牌的 QR 代码进行了鱼叉式网络钓鱼。许多组织都缺乏应用程序可见性，而且身份访问管理和单点登录 (SSO) 门户网站 (例如 Okta）暴露了端点。

利用公众应用中出现的漏洞 (T1190)（即对手利用面向 Internet 的计算机或程序中的弱点）排名第二，在 X-Force 响应过的事件中占比达 26%。这与过去的威胁情报指数报告中所称的“漏洞利用”相关联，与 2021 年的 34% 相比已有所下降。

滥用有效帐户 (T1078) 排名第三，在所观察到的事件中占比达 16%。这类事件是指对手获取并滥用现有帐户的凭证，以此获取访问权。这些事件包括云帐户 (T1078.004) (2%)、默认帐户 (T1078.001) (2%)、域帐户 (T1078.002) (5%) 和本地帐户 (T1078.003) (7%)。

信用卡信息作为网络钓鱼套件目标在 2021 年占比为 61%，2022 年降到了 29%。



## 网络钓鱼套件寿命更长，以 PII 为目标的占比超过信用卡数据

IBM Security 连续两年分析了全球数以千计的网络钓鱼套件，发现套件部署的攻击时效更长，影响的用户也更多。数据显示，所观察到的网络钓鱼套件寿命同比增加了一倍多，而整个数据集中的中值部署区间保持在相对较低的水平（3.7 天）。

总的来说，最短的部署仅维持了几分钟，而 2022 年发现的最长部署超过 3 年。我们的调查发现如下：

- 去年，部署的套件有三分之一维持了大约 2.3 天，比前一年增加了一倍多（前一年同样的比例维持了不超过 1 天）。
- 所报告的全部套件中，约有一半影响了 93 位用户，而在 2021 年，每个部署的平均潜在受害者不超过 75 位。
- 其中有份报告记载的网络钓鱼攻击的受害者总数最高刚超过了 4,000 多一点，不过这只是一个界外值。
- 数据中分析的几乎每一个网络钓鱼套件都企图获取姓名 (98%)，然后是电子邮件地址 (73%)、家庭住址 (66%) 和密码 (58%)。
- 信用卡信息作为网络钓鱼套件目标在 2021 年占比为 61%，2022 年降到了 29%。
- 网络钓鱼套件企图获取信用卡数据的占比下降表明网络钓鱼者正企图优先获取个人可标识信息 (PII)，这样他们就有更广泛和更恶意的选项。PII 能在暗网或其他论坛上收集和出售，或用于针对目标发起更多威胁攻击。

## 被欺骗的主要品牌

发现被欺骗的主要品牌大部分是最有名的科技公司。X-Force 认为，从 2021 年比较多样的品牌目标所发生的这种转变，是因为识别套件配置欺骗品牌目标（而不仅仅是默认的目标品牌）的能力提高了。许多网络钓鱼套件都为多目标，而被欺骗的品牌可通过修改一个简单的参数来实施变动。例如，一个套件默认可欺骗 Gmail，但一个单行更新就能将它变成一个欺骗 Microsoft 的攻击。

被盗凭证对于这类服务很有价值。获取受害者用来管理其所有在线信息的帐户的访问权是访问其他帐户的通道。2022 年云威胁态势报告强调了攻击者对这种初始访问的重视。该报告发现暗网上打广告销售的云帐户增量是 2021 年的三倍多 (增长了 200% 还多)。

**被欺骗的主要品牌同比概览**

| | 2022 年 | 2021 年 |
|---|---|---|
| 1 | Microsoft | Microsoft |
| 2 | Google | Apple |
| 3 | Yahoo | Google |
| 4 | Facebook | BMO Harris Bank |
| 5 | Outlook | Chase |
| 6 | Apple | Amazon |
| 7 | Adobe | Dropbox |
| 8 | AOL | DHL |
| 9 | PayPal | CNN |
| 10 | Office365 | Hotmail |

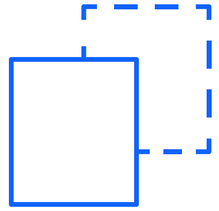
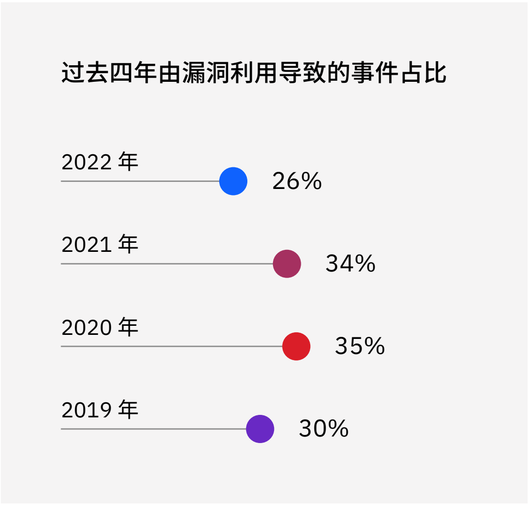


**图 3：**图表列出了 2021 年和 2022 年被欺骗的主要品牌，显示出威胁参与者越来越关注大型技术品牌。资料来源：IBM 网络钓鱼套件数据




## 漏洞

漏洞利用——2022 年被称为利用公众应用中出现的漏洞 (T1190)，是第二大感染媒介，也是攻击者自 2019 年以来更喜欢采取的入侵方法。在 X-Force 2022 年补救过的所有攻击中，漏洞利用占比达 26%（2021 年为 34%，2020 年为 35%，2019 年则为 30%）。

不是每一个威胁参与者执行的漏洞利用都会导致网络事件。2022 年由漏洞利用导致的事件数比 2021 年减少了 19%，而 2021 年则比 2020 年增加了 34%。X-Force 评估这种波动是由 2021 年底广泛传播的 Log4J 漏洞导致的。

利用漏洞进行访问是 X-Force Red 对手模拟服务团队从事的一个主要研究领域，以持续模拟高级威胁。该团队增加了对利用操作系统 (OS) 和应用程序漏洞的漏洞研究，以扩展访问和执行特权升级。这主要是源自过去与长期客户（这些客户加强了传统的活动目录攻击路径）的实践需求，以及需要探索新的攻击路径。

虽然漏洞是常见的初始访问媒介，而且行业每年都会对几大初始访问媒介进行响应，但是并非每个漏洞都是一样的。全面考虑漏洞态势并确保熟知必要背景，以了解特定漏洞对其网络造成的真正威胁，这对决策者来说很重要。

将近 30 年前，也是在常见漏洞和风险 (CVE) 系统问世之前，X-Force 就开始创建强大的漏洞数据库。该数据库现在是网络安全行业最全面的数据库之一。虽然漏洞是一个主要安全威胁，但是报告的漏洞远远多于已知的武器化漏洞利用。另外，尽管公众非常关注零日漏洞，但是已知零日漏洞总数远远少于已知漏洞总数。

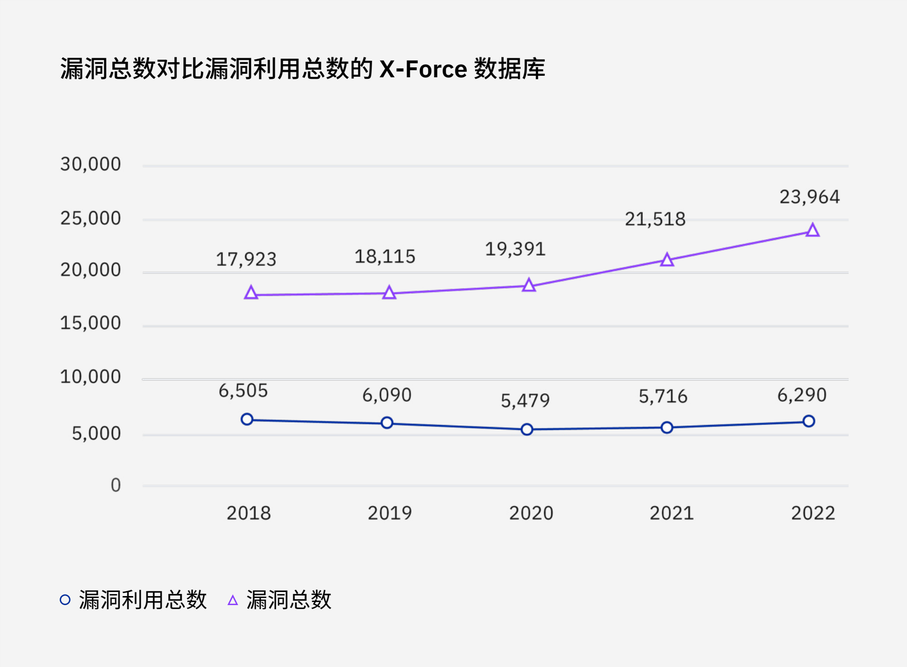



**图 4：**X-Force 漏洞数据库视图，显示了过去五年的漏洞和漏洞利用。资料来源：X-Force

每年都会发现更多的漏洞。2022 年跟踪的漏洞总数为 23,964，2021 年则为 21,518。过去十年间，漏洞数每年同比持续增长。值得庆幸的是，对漏洞数据库的分析显示，已知的可行漏洞利用在报告的漏洞中的占比近年一直在下降——2018 年为 36%，2019 年为 34%，2020 年为 28%，2021 年为 27%，2022 年则为 26%。

随着零日漏洞暴露和旧漏洞利用开发（有时是在识别旧漏洞数年后），这些数据可能会改变，而且这种下降趋势背后也存在多种可能的解释。首先，正式漏洞报告奖励计划的建立激励了大家主动发现应用程序中的漏洞。另外，已有少量广泛使用的成熟漏洞被攻击者用来利用系统漏洞，这导致威胁参与者开发新漏洞利用的需求下降。这种下降趋势很可能是多种因素综合所致，但并不代表漏洞利用的威胁性下降。

虽然漏洞利用的占比下降了，但是 X-Force 跟踪的那些漏洞利用的严重性在过去五年里一直在增加。2018 年，58% 的漏洞在通用漏洞评分系统 (CVSS) 中的严重程度评分为中等，

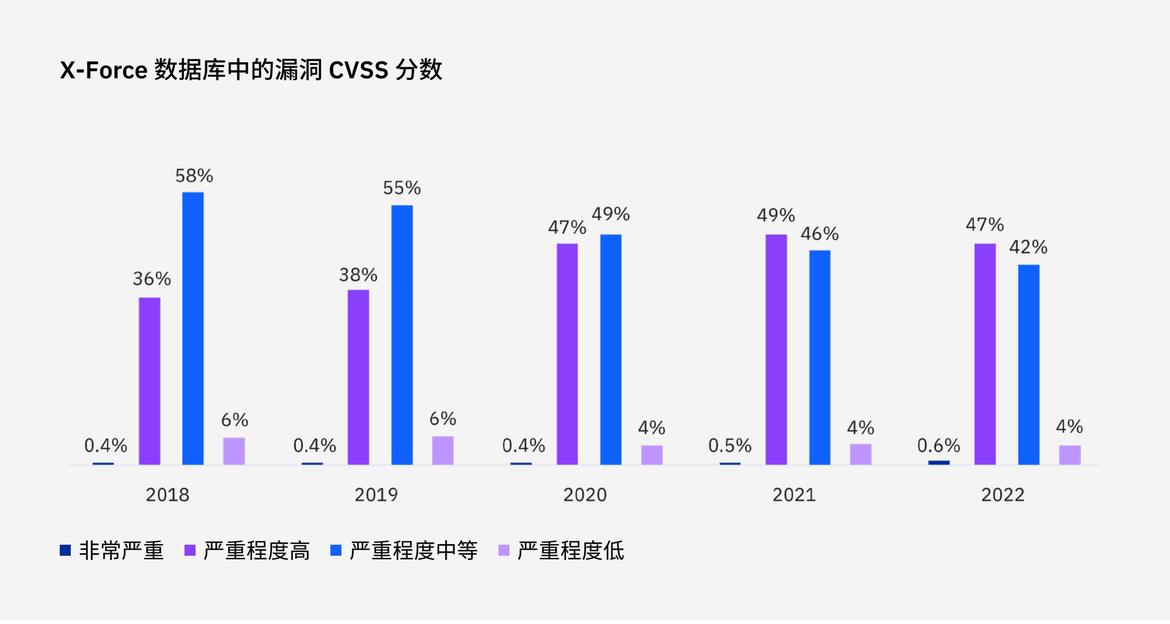



**图 5：**X-Force 漏洞数据库，显示了我们系统中跟踪的漏洞严重程度。资料来源：X-Force

即 4.0-6.9 分（总分 10 分），将近 36% 的漏洞属于高分段，即 7.0-9.9 分。现在，严重程度得分高的漏洞占比高出中分值 5%，而在 2021 年，两者的占比高低是相反的。

不过，X-Force 自 1988 年以来跟踪的所有漏洞中，有 38% 在严重性上属于高分段，仅有 1% 可列入极为严重的分数段（总分 10 分）。一半跟踪的漏洞属于严重程度的中分段，余下的 11% 可列入低分段（≤3.9 分）。仅仅是这些分数并不能反映任何 CVE 在真实世界中的严重性，因为它不能说明漏洞利用是如何完成的，甚至不能说明是否存在漏洞利用。但是，这些评分的确有助于防御者对漏洞进行比较，并优先安排以多快的速度解决它们。下页中的图 6 有助于正确理解网络安全行业面对的漏洞问题的实质情况。

## 运营技术 (OT) 漏洞

2022 年发现的工业控制系统 (ICS) 漏洞数量两年来第一次出现了下降——2020 年为 472，2021 年为 715，2022 年则降至 457。其中一个原因可能是 ICS 生命周期及其通用管理和打补丁的方式。攻击者知道，由于要求尽量少停机、设备生命周期偏长和支持数量较少的旧版软件，因此很多 ICS 组件和 OT 网络依然 存在旧漏洞风险。基础架构的使用时间常超出标准办公室工作站许多年，让特定 ICS 漏洞的寿命延长至超过那些可利用 IT 的漏洞。

**漏洞问题**

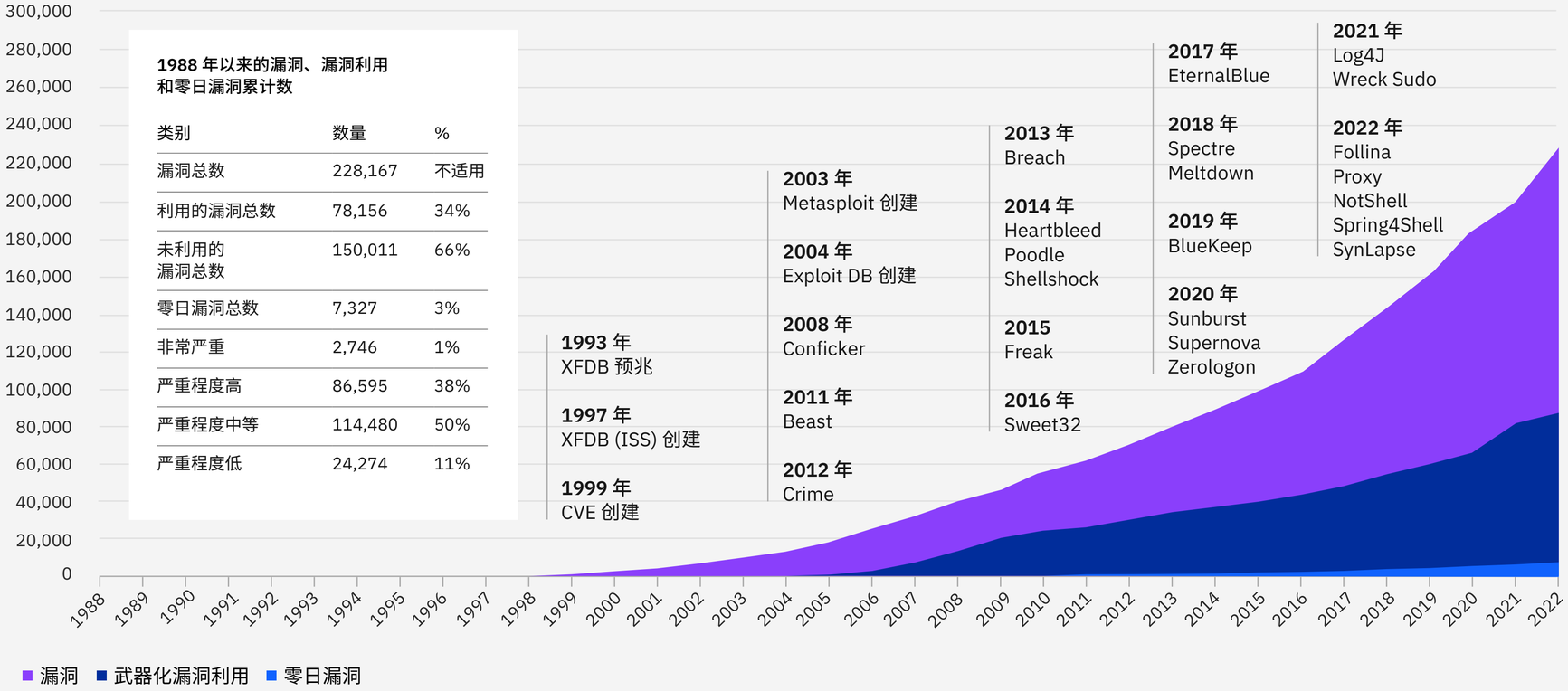



**图 6：**图形显示了 1988 年以来的漏洞、漏洞利用和零日漏洞发展，还包含了 1993 以来涉及漏洞的主事件时间线。XFDB 代表 X-Force 数据库，Exploit DB 代表漏洞利用数据库。资料来源：X-Force

# 针对目标采取的主要行动

之前，X-Force 威胁情报指数检查了主要攻击的广义类别。在 2022 年，X-Force 将此分类分为两个不同的类别：威胁参与者对受害网络采取的具体行动（或“针对目标采取的攻击行动”），以及该行动对受害者的预定或实际效果（或“影响”）。

根据 X-Force 事件响应数据显示，后门攻击部署是针对目标所采取的最常见行动，在报告的所有事件中占比高达 21%，然后是勒索软件 (17%) 和商业电子邮件泄露 (BEC) (6%)。其中每一类事件中都发现了 5% 的恶意文件 (maldoc)、垃圾邮件活动、远程访问工具和服务器访问。

**2022 年针对目标采取的主要行动**

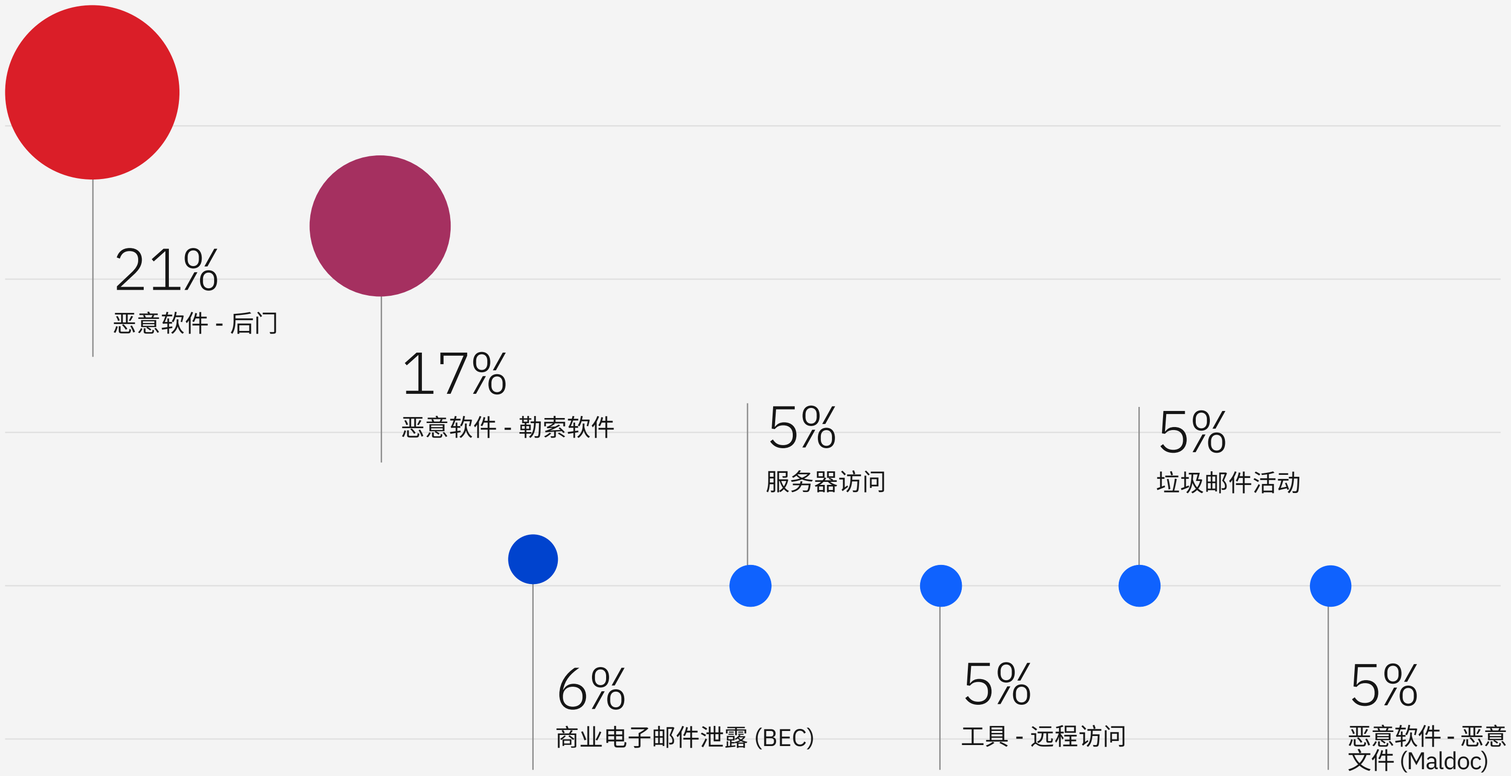



**图 7：**X-Force 2022 年针对所观察到的目标而采取的主要行动。资料来源： X-Force

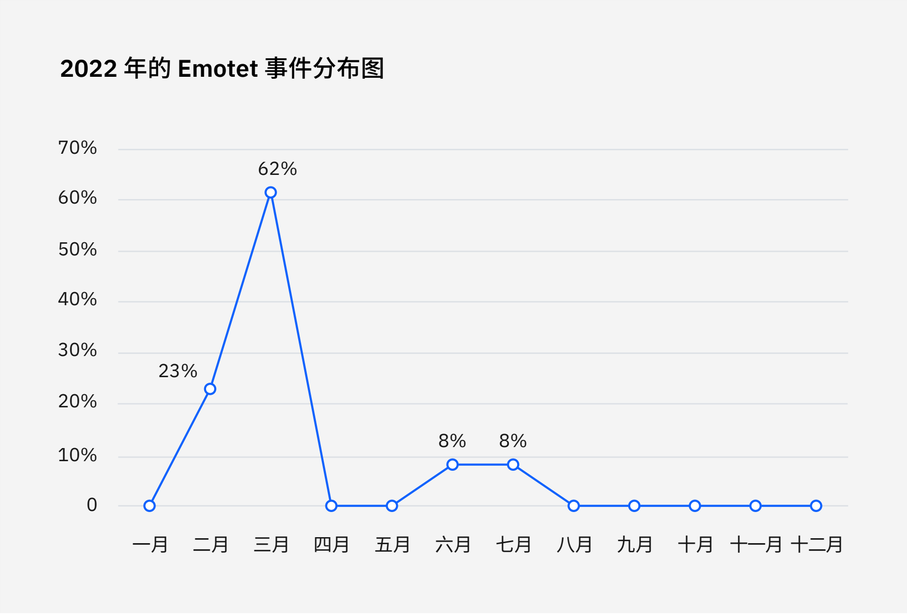


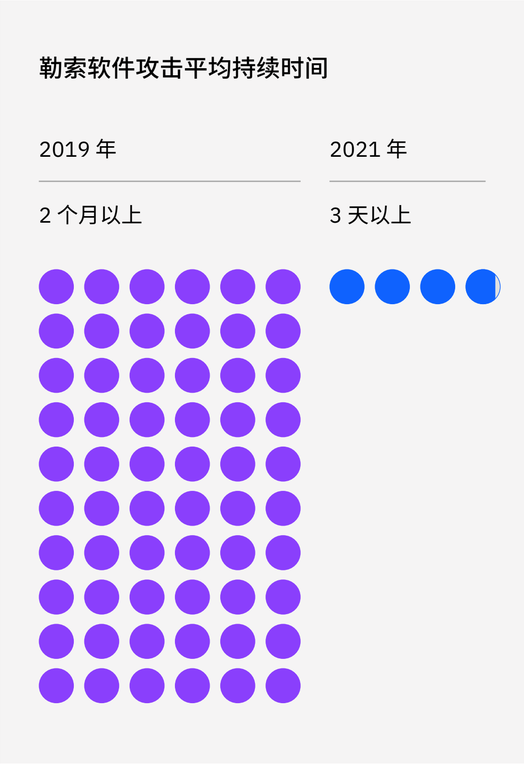

**图 8**：图形显示了 2022 年初的 Emotet 事件尖峰记录。
资料来源：X-Force

对于将后门攻击部署归类于针对目标所采取行动的事件，威胁攻击者很可能会在后门开始运行后转而实施其他攻击计划。安全团队或事件响应者的成功干预很可能阻止了威胁参与者实现更多目标。这类进一步的恶意活动很可能包括勒索软件，因为那些后门事件中有约三分之二都有勒索软件攻击的标记。

后门部署攻击占比增加还可能是因为这类访问在暗网中可带来的收益。遭受初始访问代理入侵的企业网络访问权限通常可卖到数千美元。企图快速获利的恶意参与者可能会通过避免维持访问的问题，同时横向移动并窃取高价值数据，来实施这类访问。那些缺乏必要恶意软件来建立访问的恶意攻击者可能也会寻求使用后门攻击的手段。

初始访问中介方一般会尝试拍卖他们的访问权限，X-Force 见过的售价从 5,000 到 10,000 美元不等，虽然最终价格可能会低于拍卖价。还有人曾报告访问权限的售价为 2,000-4,000 美元，有一笔甚至高达 50,000 美元。这些价格比很多其他攻击类别高很多，例如单张信用卡信息的售价曾低至不到 10 美元。

后门导致 2 月和 3 月 Emotet 事件显著爆发，这种爆发大幅提高了后门攻击事件的排名，因为在此期间部署的后门攻击占到了 2022 年识别的全球所有后门攻击事件的 47%。Emotet 从 7 月到 11 月出现了中断（在那之后又上升了接近两周时间但数量少了很多），之后相关的后门攻击事件数出现大幅下降。




## 勒索软件

而对一些攻击数量高企的勒索软件集团来说，即使在这混乱不堪的一年，勒索软件依然仅次于后门攻击部署，名列针对目标所采取的第二大攻击行动，继续对组织运营造成严重破坏。勒索软件的事件占比从 2021 年的 21% 降到了 2022 年的 17%。

IBM Security X-Force 研究显示，勒索软件攻击从 2019 年到 2021 年的平均持续时间减少了 94.34%，从两个多月缩减为不到四天。尽管如此，勒索软件目前显然是一个危险，且有迹象表明其在不断扩张，而非减速。

勒索软件操作者会通过入侵域控制器，在网络上散布其有效内容，这是一个特别具破坏性的攻击方式。有一小部分（约 4%）X-Force Red 网络渗透测试结果显示，活动目录存在错误配置的实体可能会随时受到特权升级或完全域接管的攻击。2022 年，X-Force 还观察到对底层基础架构（例如 ESXi 和 Hyper-V）出现了更凶猛的勒索软件攻击。这些攻击方法产生的潜在重大影响凸显出恰当保护域控制器和管理程序安全的重要性。

## 勒索软件变种

随着勒索软件团伙和相关访问代理变化不断，X-Force 发现活跃于此领域的主要团伙也在持续发生变动。X-Force 在 2022 年发现了 19 个勒索软件变种，而在 2021 年只发现了 16 个。LockBit 变种占到了所观察到的勒索软件总事件的 17%，2021 年仅为 7%。Phobos 和 WannaCry 并列第二名 (11%)。2022 年的主要团伙取代了 2021 年的第一团伙 REvil（也称为 Sodinokibi），2021 年制造了 37% 的事件，第二团伙 Ryuk 同年制造了 13% 的事件，而在 2022 年，两者占比都降到了 3%。

LockBit 3.0 是 LockBit 勒索软件家族的最新变种，该家族是一个与 LockerGoga 和 MegaCortex 相关联的勒索软件即服务 (RaaS) 运营商。LockBit 自 2019 年 9 月开始运营，并于 2022 年发布了 LockBit 3.0。LockBit 3.0 的大部分源代码似乎是借用了 BlackMatter 勒索软件。

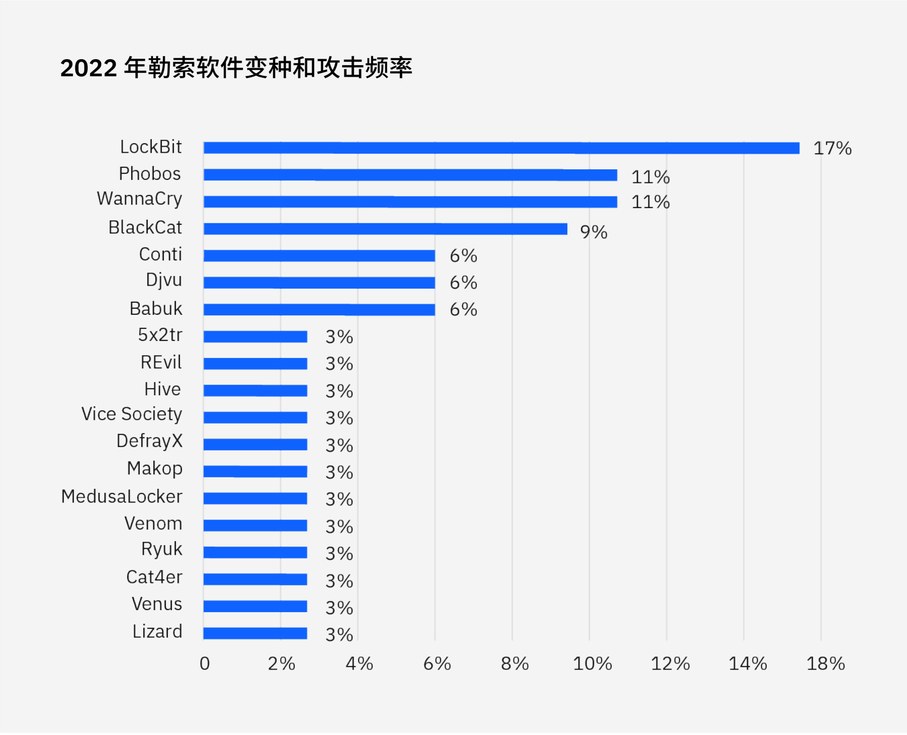



**图 9：**X-Force 2022 年事件响应参与所观察到的勒索软件变种及其攻击频率。资料来源：X-Force

研究人员最早于 2019 年初发现 Phobos 勒索软件。根据其代码、交付机制、漏洞利用技巧和赎金通知的相似性，Phobos 被鉴定为此前发现的勒索软件家族 Crysis 和 Dharma 所属的一个分支。Phobos 一般用于较小规模的攻击，所要求的赎金也较低。电子邮件网络钓鱼活动和利用易受攻击的远程桌面协议 (RDP) 端口漏洞是观察到的 Phobos 最常用传播方法。

WannaCry 最早于 2017 年发现，它使用 EternalBlue 来利用 Microsoft 服务器消息块 1.0 (SMBv1) 服务器 (MS17-010) 中的漏洞进行传播。X-Force 在 2022 年观察到的一些 WannaCry 或 Ryuk 事件都来自 3-5 年之前的感染，并发生在未打补丁的旧设备上，凸显了在此类事件后进行恰当清除的重要性。

## 商业电子邮件泄露 (BEC)

BEC 2022 年排名第三，在 X-Force 响应过的事件中占比达 6%，稍低于 2021 年 (8%) 和 2020 年的攻击占比（9%，第五名）。它取代了 2021 年的第二名攻击（即服务器访问权攻击）。这类攻击是指攻击者获取服务器访问权且最终目标未知，在 2022 年被更精确地按攻击者获取的访问权类别进行归类。在 X-Force 响应过的 BEC 事件中，有一半使用了鱼叉式网络钓鱼链接。25% 的事件采用恶意附件和滥用有效帐户进行 BEC 攻击。

06

# 主要影响

X-Force 还深入查看了事件对受害组织产生的影响，以更好地了解威胁参与者企图通过 X-Force 响应过的事件制造何种影响。组织可利用此信息更好地了解最常见的影响，以规划如何更高效地响应潜在的未来事件。

分析发现，超过四分之一的事件目的是对受害组织实施勒索，这是在 X-Force 各类修复事件中所观察到的头号影响。在观察到的勒索事件中，最常用手段是勒索软件或商务电邮泄露 (BEC) 攻击，通常包括使用远程访问工具、加密挖掘器、后门、下载程序和脚本木马。

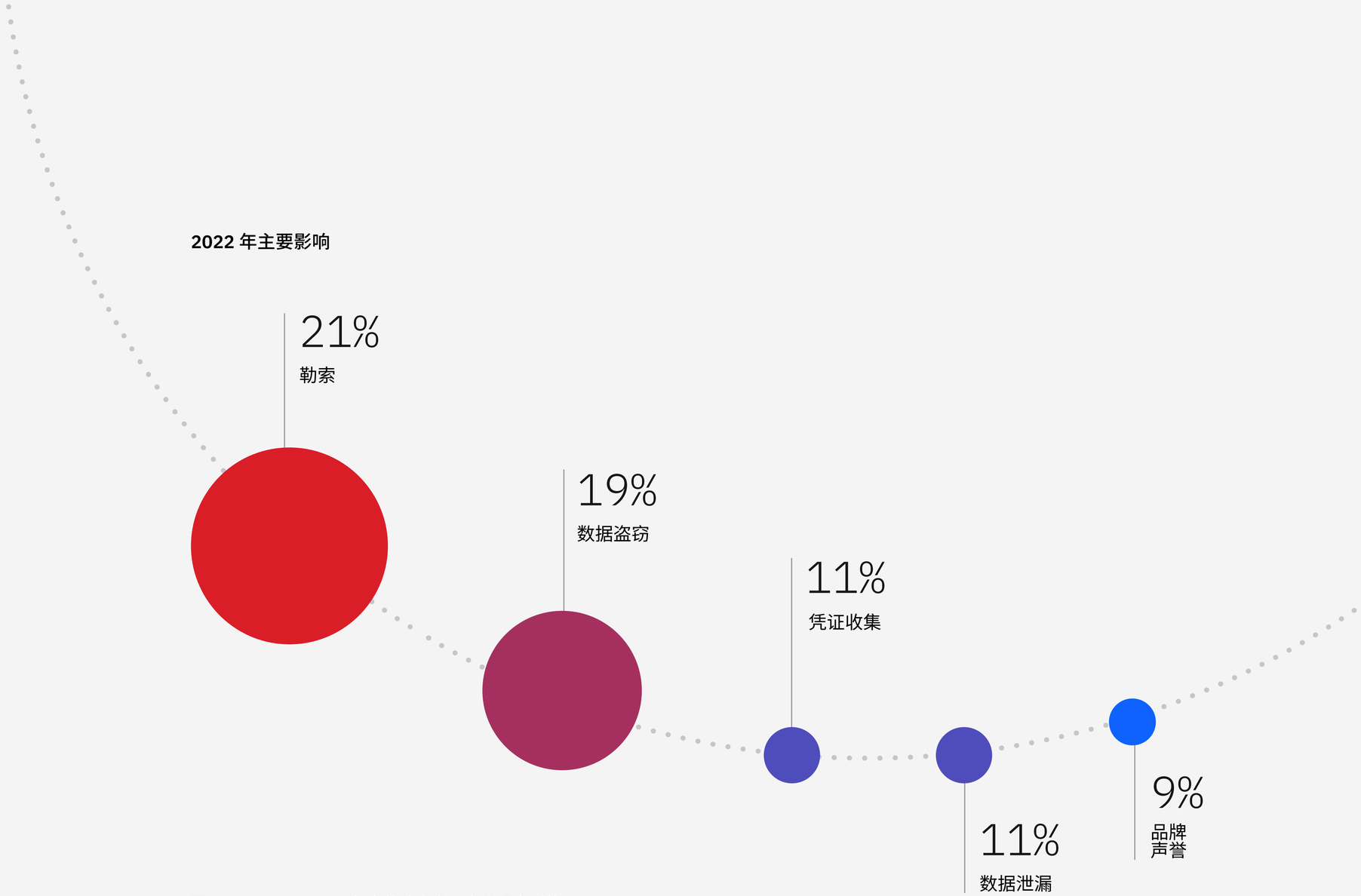



**图 10：**X-Force 2022 年事件响应参与中所观察到的主要影响。资料来源：X-Force

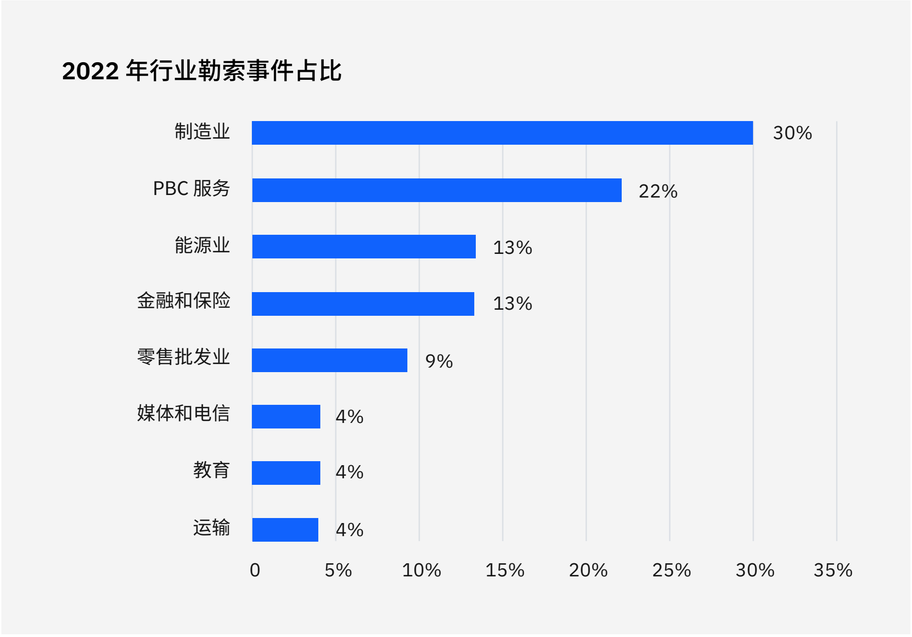



**图 11：**X-Force 2022 年事件响应参与所观察到的行业勒索事件占比 由于取整舍入，总数不及 100%。
资料来源：X-Force

数据盗窃排名第二，在 X-Force 补救过的所有事件中占比达 19%。凭证收集会导致用户名和密码被盗且需要相应的防范，占比达 11%。X-Force 能识别目的信息在被盗后确实泄漏的事件占比低于数据盗窃，仅为 11%。品牌声誉影响（例如破坏客户为其顾客提供的服务）的事件占比为 9%。请参阅附录，查看 X-Force 跟踪的完整影响列表。影响受害者品牌声誉的事件主要是分布式拒绝服务 (DDoS) 攻击，这也常用于勒索受害者支付金钱来停止攻击。

**网上敲诈勒索的重大发展动态[1-9]**

| 年份 | 事件 | 策略 |
|---|---|---|
| 2013 年 | Cryptolocker - 首批主要的勒索软件爆发之一 | 数据加密 |
| 2014 年 | DDoS 4 Bitcoin、Armada Collective | 赎金 DDoS |
| 2015 年 | Chimera 勒索软件增加要在网上泄漏被盗数据而产生的威胁 | 双倍勒索 |
| 2017 年至 2018 年 | BitPaymer 和 SamSam | 大狩猎攻击 |
| 2020 年 | Vastaamo 勒索软件事件 | 三倍勒索 |

## 勒索

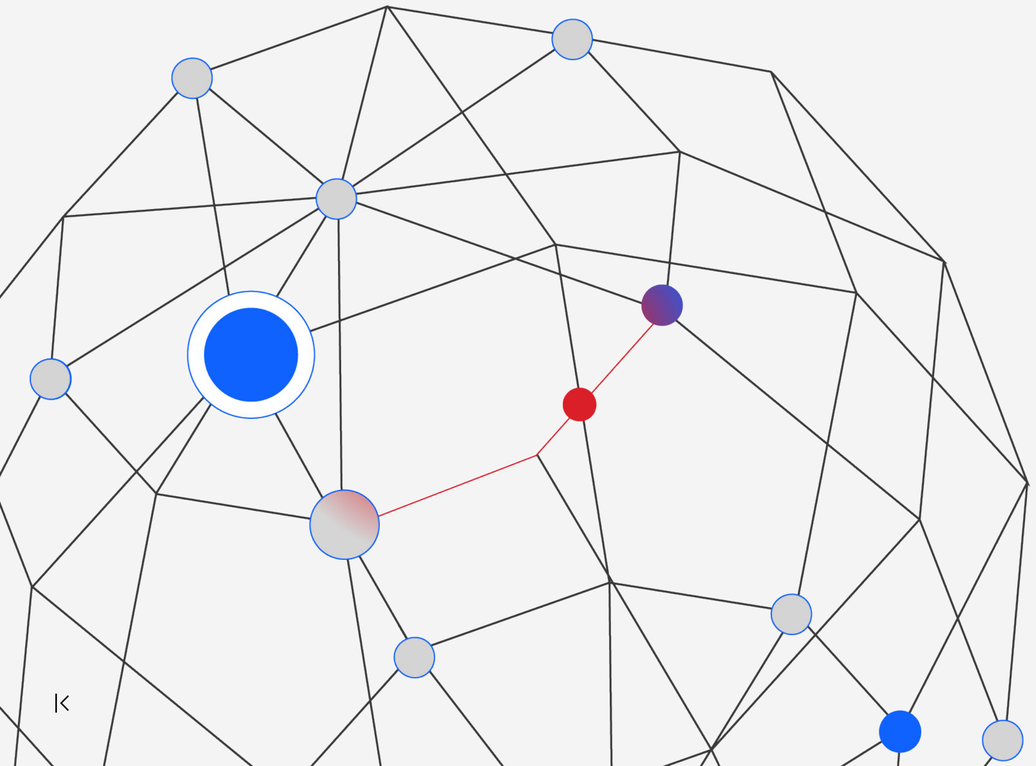
虽然勒索现今最常与勒索软件相联系，但是勒索活动包含了各种方法，来对其目标施压。这些方法包括 DDoS 威胁、加密数据，以及最近出现的双倍和三倍勒索威胁并结合了此前见过的一些元素。

2022 年，至少有一个勒索软件团伙开始尝试的另一个策略就是让下游受害者更轻松地访问他们之前已盗窃的数据。通过让间接受害者更轻松地在数据泄漏中识别其数据，攻击者是企图对勒索软件团伙或附属团伙从一开始就针对的目标组织增加后续压力。X-Force 预计 2023 年会看到威胁参与者尝试采用增强的或全新的下游受害者通知，来增加入侵带来的潜在法律和声誉代价。

网络攻击的防御者和受害者通常都会关注威胁参与者对组织造成的、所观察到的影响。但是，很重要的一点是要考虑威胁参与者的目的和能力及其随时间的演变趋势。这种方法能更好地识别下一波可能出现的能力演变。考虑到不断扩展的勒索选项和勒索软件参与者的主要目标（经济获益），X-Force 团队估计威胁参与者将继续演变并扩展其勒索方法，以找到新的方式来对受害者施压而让其付款。

07

# 俄乌战争与网络相关的发展动态



在俄罗斯入侵乌克兰之后，由俄罗斯政府支持的网络活动（截至本文发表之时）仍未造成西方政府实体最初所恐惧的广泛且具有高度影响的攻击。但是，俄罗斯已针对位于乌克兰的目标部署了空前数量的擦除式恶意软件，凸显出该国在持续增强破坏性恶意软件能力。另外，该入侵已导致由同情各方的团伙发起的黑客行为主义者活动的复兴，以及带来针对东欧网络罪犯态势的重组活动。

考虑到俄罗斯自 2015 年以来展现出的对关键基础架构进行网络攻击的超高能力，国际网络安全机构发出了一份警告（2022 年 4 月）。警告中提到了潜在的重大网络行动，以及在乌克兰和其他地方的相关破坏。X-Force 估计已出现的最严重威胁包括黑客行为和擦除式恶意软件的复兴，以及网络罪犯世界的巨大改变。这些行动大多数都是攻击位于乌克兰、俄罗斯和邻近国家/地区的实体，但有些也传播到了其他地区。

另一方面，防御者正熟练地使用过去几年在检测、响应和信息分享方面取得的发展。许多早期发起的擦除式恶意软件攻击都已被快速识别、分析和宣传。这些攻击包括至少八种已识别的擦除式恶意软件，以及发现和破坏一次俄罗斯所计划的对乌克兰电网实施的网络攻击（2022 年 4 月）。

# 俄乌战争与网络相关的发展动态

在网络空间中，这场持续战争的最广泛影响来源于自称为黑客行为主义者的团伙，他们以黑客行动支持乌克兰或俄罗斯的国家利益。自俄罗斯入侵以来形成了许多团伙，他们正对俄罗斯和乌克兰的网络发起攻击，以表明政治观点，其中 Killnet 是最活跃的同情俄罗斯的团伙之一。它声称对位于北大西洋公约组织 (NATO) 成员国、欧洲同盟国，以及日本和美国的公共服务、政府部门、机场、银行和能源公司发起了 DDoS 攻击。符合 Killnet 目标对象的实体应考虑确保有 DDoS 缓解措施，例如使用第三方 DDoS 缓解提供商的服务。

**2022 年重要黑客行为主义者事件时间线**

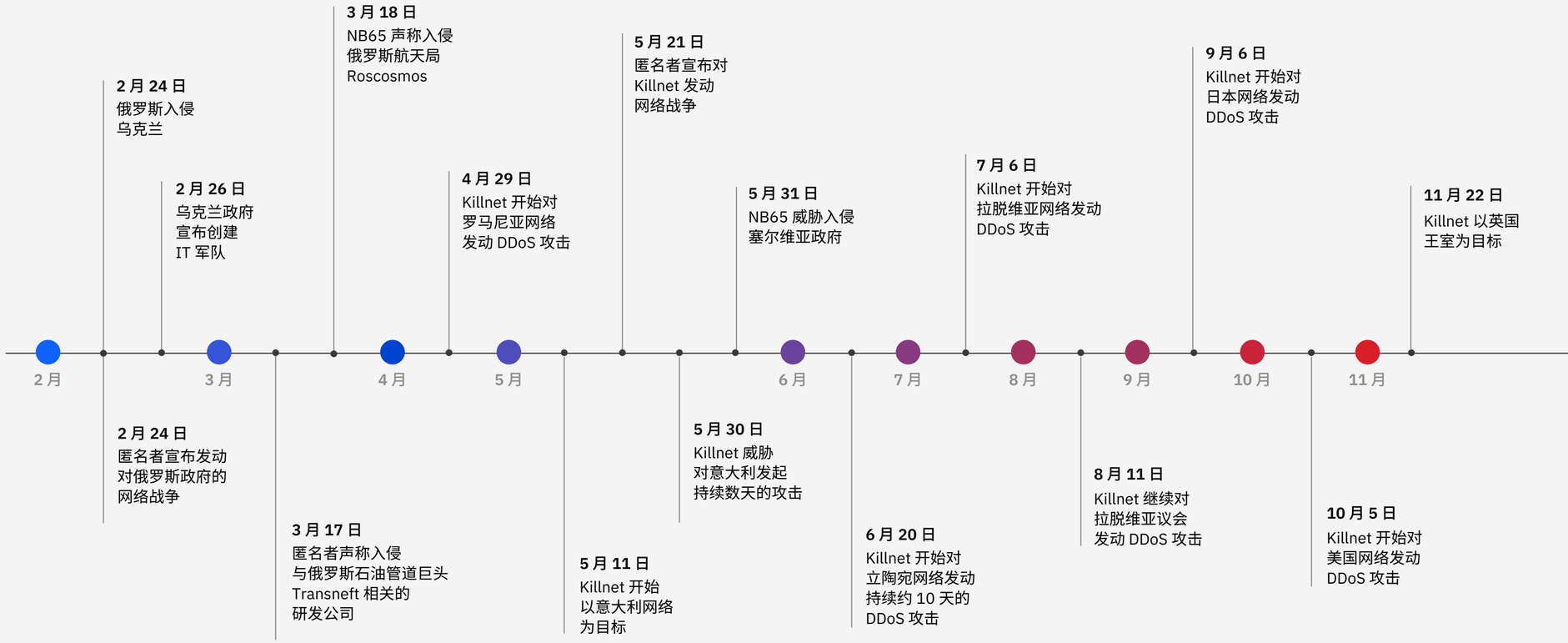



**图 12：**图片显示了迄今为止观察到的乌克兰冲突期间属于黑客行为主义者的各类事件。资料来源：X-Force 开源报告分析

## 俄乌战争中使用的擦除式恶意软件

俄乌战争的特点之一是以前所未有的规模，针对多个目标连续快速地使用了多个擦除式恶意软件家族，以及在实施活跃的军事行动的同时使用恶意软件。

这些部署包括至少九种新式擦除式恶意软件：AcidRain、WhisperGate、HermeticWiper、IsaacWiper、CaddyWiper、DoubleZero、AwfulShred、OrcShred 和 SoloShred。这些擦除式恶意软件主要用于攻击乌克兰网络，始于入侵之前，一直延续到战争的前期阶段（主要是 2022 年 1-3 月）。虽然过去也有人使用过擦除式恶意软件，但大多数是单独用于针对有限的目标群体。

然而，WannaCry 和 NotPetya 明显是个例外，它们在攻击了初始受害者之后进行了任意传播，因此人们担忧此类擦除式恶意软件会得到更广泛的传播，或用于在其他地方实施恶意行动。

X-Force 继续认为俄罗斯政府支持的网络威胁参与者依然对全球计算机网络和关键基础架构造成巨大的威胁。 这一判断是基于俄罗斯针对乌克兰、欧洲、NATO 和美国网络的长期网络行动，以及俄罗斯威胁团伙自 2015 年以来执行的攻击行动。

## 俄罗斯网络犯罪团伙剧变

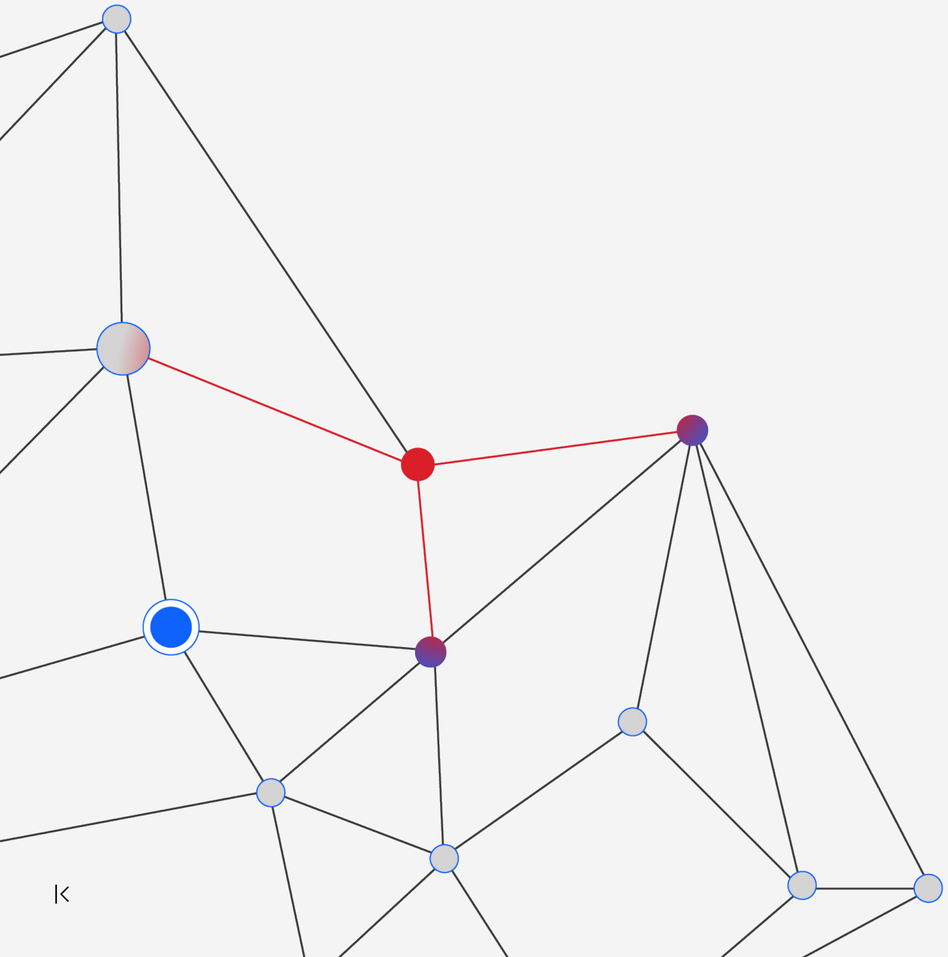
2022 年对 ITG23 来说是一个动荡之年，它是俄罗斯最著名的网络罪犯集团之一，主要因开发了 Trickbot 银行特洛伊木马和 Conti 勒索软件而闻名。在公开表示支持俄罗斯入侵乌克兰之后，该团伙在 2022 年初经历了一系列备受瞩目的泄漏。这些泄漏被称为 ContiLeaks 和 TrickLeaks，导致公布了成千上万条聊天信息和对许多团伙成员的人肉搜索。X-Force 发现的证据表明 ITG23 从 2022 年 4 月中旬就开始了系统化攻击，并至少延续至 6 月中旬——这是一个前所未有的转变，因为该团伙此前从未以乌克兰为攻击目标。

另外，该团伙似乎已停止使用其最知名的恶意软件家族 Trickbot 和 Bazar，并停止了其 Conti 勒索软件行动。各种报告显示，该团伙可能出现了重大的人事调整，分裂成了数个派系，有些成员甚至彻底离开了。

在 2021 年造成了海量感染的 Trickbot 和 Bazar 被关停所导致的空白迅速被 Emotet、IcedID、Qakbot 和 Bumblebee 等恶意软件家族填补。在关停前，ITG23 依然在大量部署 Conti 勒索软件，其数量在 X-Force 2022 年第一季度响应过的所有勒索软件事件中占到了三分之一。

该团伙还发布了新版的 Anchor 恶意软件，这是该团伙传统上一直针对高知名度目标部署的秘密后门。X-Force 发现了这个更新的版本，它名为 AnchorMail，拥有新型的基于电子邮件的指挥控制 (C2) 通信机制。C2 服务器使用简单电子邮件传输协议 (SMTPS) 和互联网消息访问协议安全 (IMAPS) 协议，恶意软件则通过发送和接收专门编写的电子邮件消息来与服务器通信。

# 恶意软件态势



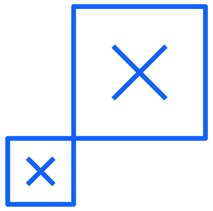
## 通过 USB 传播的蠕虫数增加

在 X-Force 于 2022 年 5 月中旬观察到 Raspberry Robin 针对组织的感染攻击之后，这款神秘的蠕虫就开始因用户分享通用串行总线 (USB) 设备而在受害者的网络中快速传播。这波感染在 6 月初达到高峰，到 8 月上旬，Raspberry Robin 在 X-Force 所观察到的感染攻击中占比达 17%。该峰值出现在油气业、制造业和运输业中。17% 的感染攻击率对这些行业来说是非常高的，因为一共只有不到 1% 的 X-Force 客户见过同款恶意软件。X-Force 还观察到 2022 年 9-11 月出现了更多 Raspberry Robin 活动。

基于 USB 的蠕虫传播通过社会工程实现，并需要通过一些物理方式访问网络或端点来成功实施感染，无论是通过合法用户还是其他途径。X-Force 建议确保您的安全工具阻止已知基于 USB 的恶意软件、进行安全意识培训，并对任何移动介质禁用自动运行功能。在特别敏感的环境（例如 OT 或存在气隙的环境）中，完全禁止使用 USB 闪存盘是最安全的做法。如果有必要使用此类设备，那么除了实施上述建议外，还必须严格控制在您的环境中使用批准的便携式设备数量。

## Rust 增加

2022 年期间，Rust 编程语言越来越得到恶意软件开发者重视和采纳，因为它拥有跨平台支持，且防病毒检测率比其他更常用的编程语言低。与 Go 语言相似，它也受益于更复杂的编译过程，这一过程会让逆向工程分析恶意软件时更耗时。多个勒索软件开发者发布了其恶意软件的 Rust 版，包括 BlackCat、Hive、Zeon 和最近的 RansomExx。另外，X-Force 还分析一款以 Rust 编写的 ITG23 加密器，以及 CargoBay 家族的后门和下载程序。Rust 的欢迎度上升凸显出整个勒索软件生态系统一直持续关注通过创新来逃避检测的方法。



## Vidar InfoStealer

X-Force 注意到从 2022 月 6 月开始突然出现大量 Vidar InfoStealer 恶意软件攻击，一直持续到 2023 年初。第一次发现 Vidar 是在 2018 年，这是一款恶意信息窃密特洛伊木马，通过恶意软件即服务 (MaaS) 传播。该特洛伊木马常常通过用户点击恶意垃圾邮件 (malspam) 链接或附件来执行。Vidar 功能集广泛，因此可用于检索各种设备信息，包括信用卡信息、用户名、密码和文件，以及对用户的桌面截图。Vidar 还能窃取比特币和以太坊加密货币钱包。

通过信息窃密恶意软件 (info stealer) 进行的攻击一般都以金钱为目的。软件会分析被盗数据、整理任何有价值的信息并将其纳入数据库。然后，该数据库就会在暗网或通过私人消息应用程序 Telegram 出售。威胁参与者可能会使用这些信息进行各种欺诈，例如申请银行贷款或信用卡、线上购物或伪造健康保险索赔。

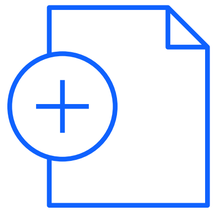
威胁参与者能使用泄露的登录凭证来访问企业帐户和远程服务。使用信息窃密恶意软件的费用约为每月 250 美元，而且用户可自行决定部署哪种恶意软件。X-Force 经常看到有市场尝试出售透过信息窃密恶意软件窃取的访问权，售价为 10-75 美元。获取访问权后，威胁参与者就能轻松使用被入侵的帐户特权作为起点，来进行更多恶意活动。

## 恶意软件交付机制的演变

恶意软件越来越经常通过附于网络钓鱼电子邮件恶意 Microsoft Office 文件传播。恶意软件开发者创建了这些包含恶意宏的文件，旨在于文件打开时执行恶意软件。宏的此类应用变得非常广泛，因此 Microsoft Office 产品开始在打开启用宏的文件时加入安全警告。2022 年 7 月，Microsoft 开始在通过电子邮件或互联网接收到的文件中默认阻止宏执行。

随着防御者的检测和预防能力增强，威胁参与者开始逐渐弃用 Visual Basic 应用程序 (VBA)，而改用 Microsoft Excel 中现有的旧版宏格式 (Macro 4.0)。恶意 Excel 文件的应用已有一段时间，但是 Excel 文件中的大多数安全机制都是围绕 VBA 宏构建的。有一段时间，Excel Macro 4.0 宏是一种有效逃避检测的方式。同期，一些威胁参与者开始在电子邮件中发送链接，将受害者引至病毒释放木马 (dropper) 网站下载恶意文件，而非直接将其作为邮件附件发送。随着 Microsoft 做出更改，让管理员能够禁用 Macro 4.0 和阻止执行从互联网上下载的宏，威胁参与者不得不再次改变策略。

在 Microsoft 做出更改后，许多恶意软件作者依然使用启用宏的 Microsoft Office 文件，但高级团伙则采用了一条更加错综复杂的感染链。这些较新的策略包括综合嵌入了二进制的 HTML 文件或受密码保护的压缩文件。那些文件还包括一个 ISO 映像文件，其中可能包含一个不太可能发送给电子邮件接收人或通过互联网下载的 LNK 文件、CMD 文件或其他文件类型。其他则包括远程模板注入或漏洞利用。 CVE-2021-40444 是 Microsoft HTML (MSHTML) 中的一个远程代码执行漏洞，是使用软件组件在 Microsoft Windows 中呈现网页，以执行恶意软件，而非依靠宏执行恶意软件的例子。



## 垃圾邮件数据凸显出勒索软件威胁，并进一步展现出宏趋势的作用

X-Force 分析了网络钓鱼和垃圾电子邮件的趋势，以更好地了解其整体效果和威胁参与者对它们的使用。调查发现，垃圾电子邮件全年常用于传送经常导致勒索软件感染恶意软件，例如 Emotet、Qakbot、IcedID 和 Bumblebee。

| 恶意软件[10-18] | 勒索软件 |
|---|---|
| *Trickbot* | *Conti* |
| *Bazarloader* | *Conti*、Diavol |
| IcedID | *Conti*、Quantum |
| Bumblebee | *Conti*、Diavol、Quantum |
| Emotet | *Conti*、BlackCat、Quantum |
| Qakbot | *REvil*、*Conti*、Black Basta |
| SocGholish | LockBit |

此表中的数据涵盖 2021 年末至此报告发布之日。
斜体部分表示 2022 年出现过，但 X-Force 至少在 2022 年 10 月之前未曾观察到的恶意软件或勒索软件。

X-Force 发现，使用 HTML 走私入侵受害者的 Qakbot 活动在 2022 年 9 月激增。那些感染关联着广泛的入侵后活动，包括侦察、信息收集和部署更多有效内容。2022 年未经检查的 Qakbot 感染导致了多个 Black Basta 感染。X-Force 发现，在 Qakbot 2022 年夏季的网络钓鱼活动中断期间，Black Basta 勒索软件团伙的泄露网站上声称发动的勒索软件攻击明显减少。X-Force 预计 Qakbot 活动的恢复也将导致出现更多勒索软件受害者。

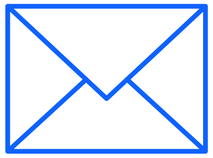
## 绕过宏

为了应对 Microsoft 从 2021 年 10 月开始做出的宏更改，攻击者开始使用 ISO 和 LNK 文件来作为感染受害者组织的重要策略。此策略包括通过容器文件直接交付其有效负载内容，以及加密其中启用宏的文件。

- ISO 文件和压缩文件正被用于绕过 Microsoft 用来帮助目标启用恶意宏的网络标记 (MOTW) 属性。虽然 ISO 或压缩文件会看起来像是从互联网上下载的，但其中启用宏的附件则不会，这就能让威胁参与者能够继续这类攻击。
- 另一种绕过宏限制的方式是直接在 LNK 文件中包含有效内容，这些文件在点击后就会执行主要用于下载或加载后续阶段的任意命令。2022 年初之前，只有 2021 年 2 月的一个活动使用了此策略。X-Force 首次发现此策略的实施是在 2022 年 2 月下旬至 3 月，但现在发现它的频率很高。

X-Force 在威胁参与者的垃圾邮件活动中检测到的其他趋势包括越来越多地使用已加密压缩归档作为附件和线程劫持（如此处所释)。

- 防病毒软件更难以检测和标记为恶意的已加密压缩扩展在 2022 年的应用也增加了。与 2021 年 4 月之后的同年数据相比，有此类附件的垃圾电子邮件每周平均数在 2022 年增加了 9 倍。
- 线程劫持是一种用于增加垃圾邮件合理性并更有效地诱使受害者参与的长期策略，威胁参与者会将自己融入现有电子邮件线程中。与 2021 年的大多数相比，此策略在 2022 年的应用明显增加，并在春季之前逐渐减少。X-Force 估计主要是 Emotet 垃圾技术导致了这一趋势。



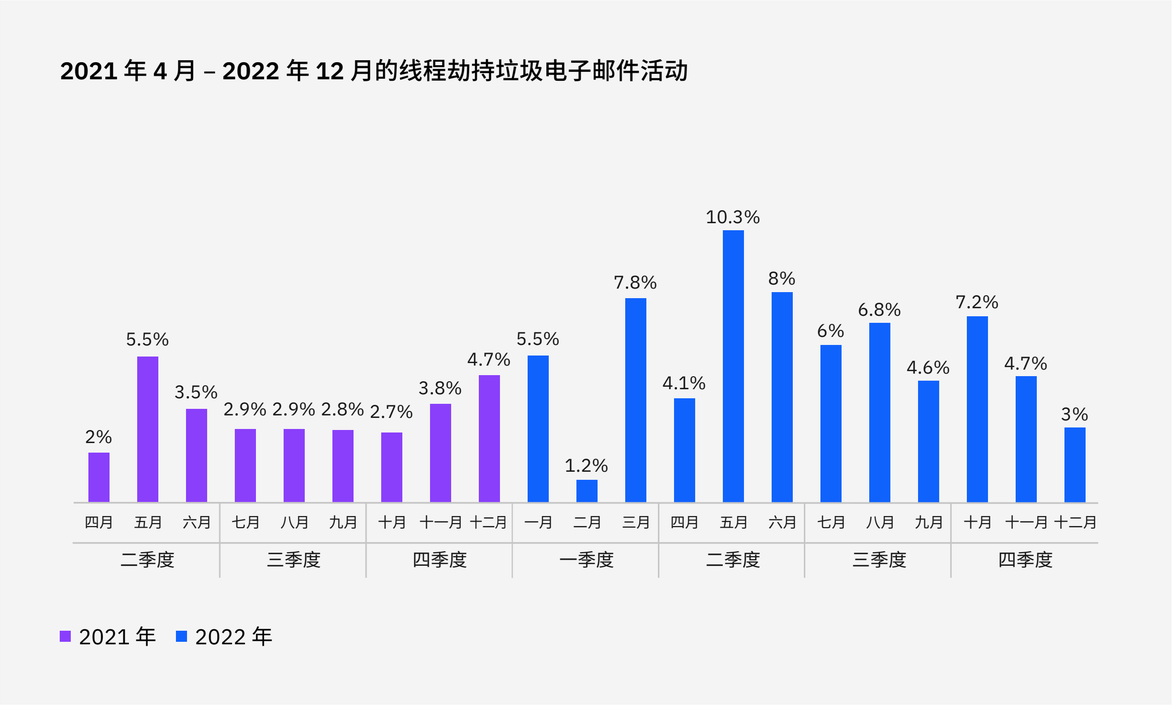



**图 13：**图形显示了 X-Force 从 2021 年 4 月之后的数据检测到的线程劫持攻击总数的月百分比。
资料来源：X-Force

– 自从僵尸网络于 2021 年 1 月中断后，Emotet 于 2021 年 11 月回归。它的活动继续到 2022 年，在 7 月中旬开始了将近 4 个月的中断，然后在 2022 年 11 月回归了将近两周。

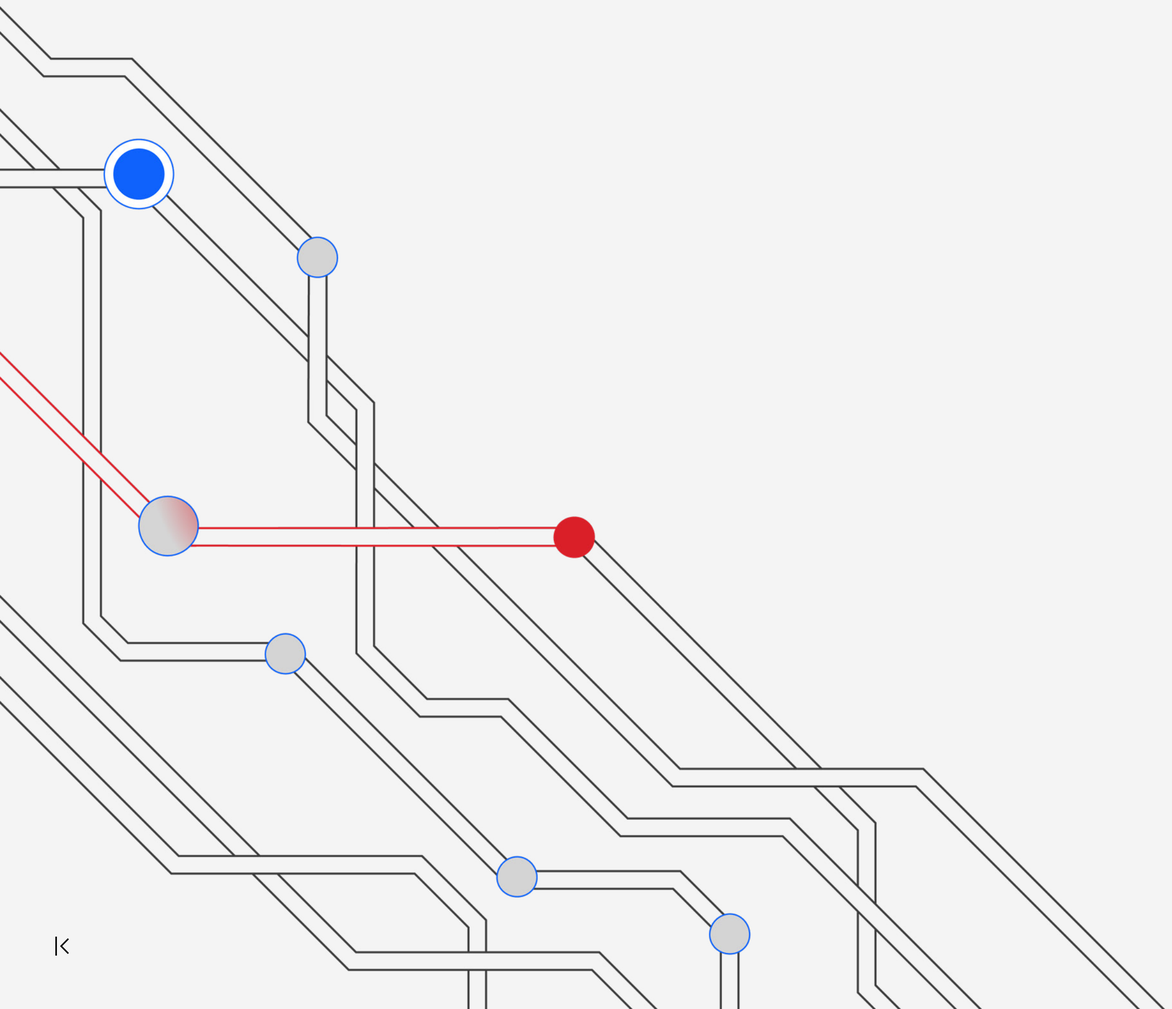
– 数据显示，与 2021 年 4 月之后的可用数据相比，2022 年的每月攻击次数增加了约一倍。线程劫持在 2022 年 5 月之前呈不稳定的变化趋势，而下半年的下降趋势大致与 Emotet 的不活动状态相呼应。可导致 Emotet、Qakbot 和 IcedID 感染的垃圾电子邮件都大量使用了线程劫持手段。

– Emotet 在 2021 年 11 月的回归导致形成了 2022 年 5 月之前的不稳定上升趋势。下半年的整体下降趋势与 Emotet 从 2022 年 7 月到 10 月出现的中断以及 11 月的短暂回归相呼应。

– 跟踪线程劫持并准确将它与威胁参与者仅为垃圾电子邮件添加一个回复主题行标题的情况相区别很困难，并且以后很可能会变得更加困难。例如，一些威胁参与者已开始删除“Re:”主题行标题，这很可能是因为他们意识到这些标题可用于跟踪其活动。

09

# 对 OT 和工业控制系统的威胁



## 对运营技术的威胁

2022 年发现了两种新型特定 OT 恶意软件 Industroyer2 和 INCONTROLLER（也称为 PIPEDREAM），以及许多 OT 漏洞（称为 OT: ICEFALL）。OT 网络威胁态势正在急剧扩大，OT 资产所有者和运营商需要敏锐地意识到态势的改变。

X-Force 深入探索了特定 OT 的网络攻击和 IR 数据，以帮助获得关于威胁参与者企图如何入侵 OT 相关行业客户的洞察成果。网络攻击数据显示：强力攻击、使用偏弱和过时的加密标准与弱密码或默认密码都是这些行业 IT 和 OT 环境中的常见警报。

表示可能发生强力攻击的警报最常见于特定事故指挥系统 (ICS) 的攻击数据，紧随其后的是弱加密警报。最常见的弱加密警报是关于持续使用已于 2021 年 3 月弃用的过时和不安全加密方法：传输层安全性 (TLS) 1.0。虽然美国政府建议重新配置使用 TLS 1.2 或 1.3，但是美国国家标准技术学会 (NIST) 指南更深入地谈论了常见的现实问题。现实问题就是旧系统可能需要继续使用较弱版的加密，以确保功能持续可用。

弱密码或默认密码警报也很突出，尤其是考虑到这些都是基本的各类配置漏洞，可让攻击者更易发动强力攻击。广泛且很可能无差别的内部和外部漏洞扫描是针对 OT 相关行业的最常见攻击。数据显示旧漏洞和威胁如今依然相关。Cisco Talos 在 2021 年发现的一组 Advantech R-SeeNet 监控软件漏洞触发了 2022 年整个 OT 行业微弱多数的漏洞扫描警报。这些漏洞可能会让攻击者能够执行任意代码或命令。

但是，第二常见的漏洞可追溯到 2016 年：Trihedral VTScada 应用程序 CVE-2016-4510 中的一个过滤器绕过漏洞，它可让未经授权的用户能够发送访问文件的 HTTP 请求。进一步凸显出旧威胁风险的是继续对 OT 存在巨大威胁的攻击类型，例如 WannaCry 和 Conficker。

## 制造业依然是最大的 OT 行业目标

纵观与运营技术 (OT) 相关行业的事件子集，数据显示制造业是 2022 年最大的攻击目标。在 X-Force 协助补救过的事件中，有 58% 的受害者是制造业。部署后门攻击是针对目标采取的首要攻击行动，在制造业安全事件中占比达 28%。勒索软件参与者尤其以此行业作为目标，原因很可能是这些组织对停机的容忍度低。

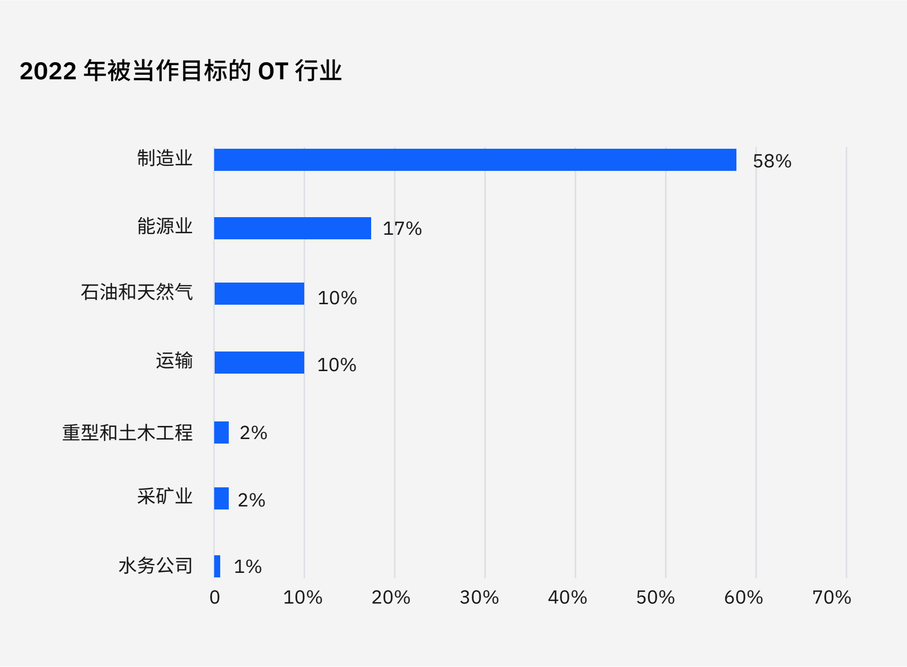



**图 14：**X-Force 2022 年响应过 IR 事件 OT 相关行业占比。
资料来源：X-Force

纵观 OT 相关行业事件的各类初始访问媒介，鱼叉式网络钓鱼的事件占比达 38%，包括使用附件 (22%)、使用链接 (14%) 和服务伪装鱼叉式网络钓鱼 (2%)。利用公众应用中出现的漏洞排名第二，占比达 24%，与更广泛的行业趋势相符。后门侦测也在这些行业的安全事件中排名靠前 (20%)，然后是勒索软件 (19%)。勒索的影响排名仍居首位，事件占比达 29%，紧接其后的是数据盗窃 (24%)。

运营技术 (OT) 中另一个被利用的主要漏洞是 OT 和 IT 网络之间缺乏恰当的分段隔断。X-Force Red 对手模拟服务的团队会定期以弱分段为目标，以获取 OT 隔离环境的访问权限。这些环境包括以跳板机、双宿主操作员工作站和报告服务器为目标，例如向企业 IT 网络暴露 OT web 和 SQL 服务的数据历史数据库。对您网络中的这些部分进行恰当分段并紧密监控其中的通信可以保护资产安全。

# 地理趋势

亚太地区在 2022 年已连续两年成为受攻击最严重的区域，在 X-Force IR 响应过的事件中占比达 31%。欧洲紧随其后 (28%)，然后是北美 (25%)。亚太地区和欧洲的事件占比较高，与 2021 年的数据相比分别上升了 5% 和 4%，而中东的事件则从 14% 大幅下降到了 4%。

**2020 – 2022 年事件区域占比**

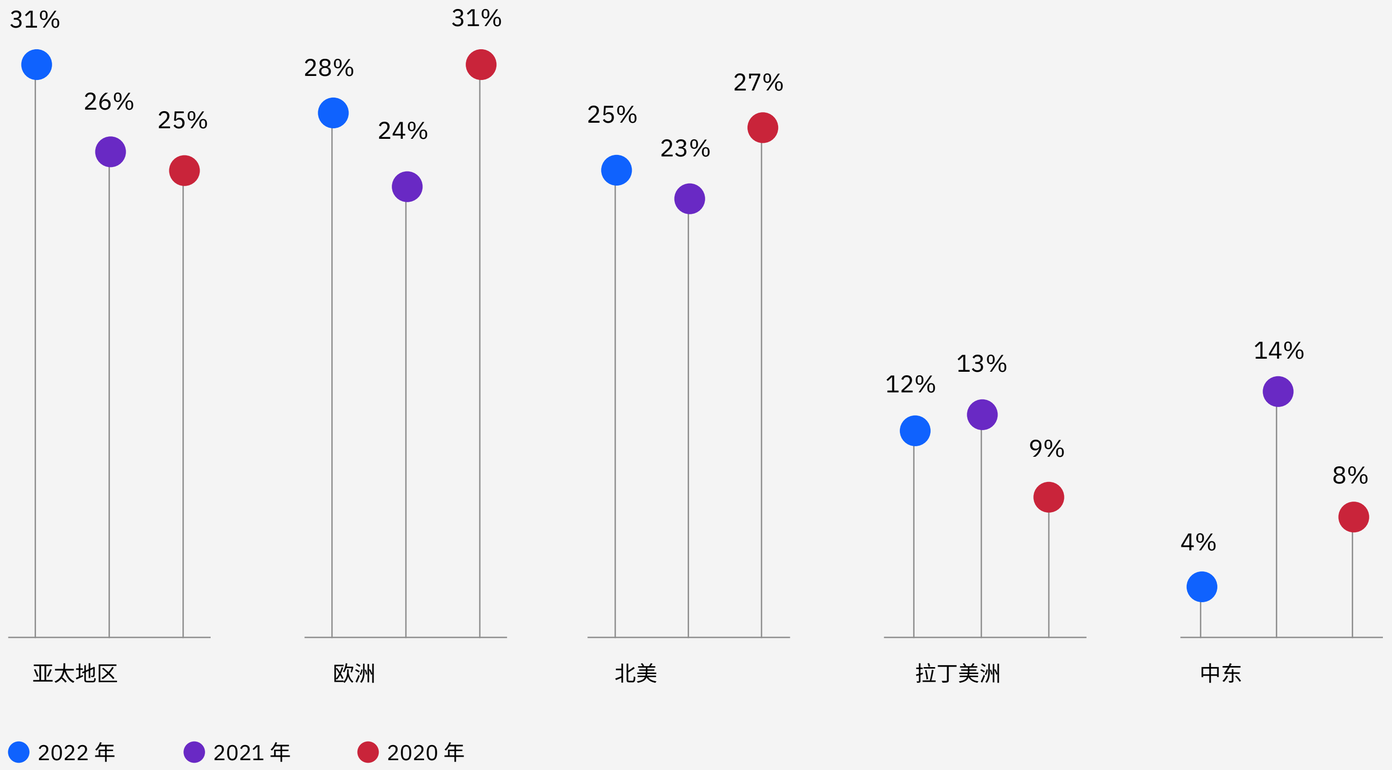



**图 15：**X-Force 2020-2022 年响应过的 IR 事件区域占比。资料来源：X-Force

## #1 | 亚太地区

亚太地区，尤其是日本，是 2022 年 Emotet 爆发的中心。虽然不是与欧洲的战争直接相关，但是 Emotet 事件在日本激增的时间与俄罗斯入侵乌克兰的时间同步，网络安全社区的其他研究人员指出这在当时大幅推动了 Emotet 活动的爆发。在数个行业中都发现了垃圾邮件活动，其中最多的是制造业和金融与保险业。Emotet 主要通过使用引人注意的标题的垃圾邮件活动传播。

制造业是此区域受攻击最严重的行业，威胁事件占比达 48%，金融与保险业排名第二但占比少了很多，达 18%。

藏匿于附件中的鱼叉式网络钓鱼是此区域的主要感染媒介 (40%)，然后是利用面向公众应用程序中出现的各类漏洞 (22%)，外部远程服务和鱼叉式网络钓鱼链接并列第三名 (12%)。

部署后门攻击是该区域针对目标采取的首要行动，事件占比高达 31%，勒索软件排名第二 (13%)，恶意文件 (maldoc) 排名第三 (10%)。勒索是所观察到的最常见影响，事件占比达 28%，对品牌声誉的影响排名第二 (22%)，数据盗窃排名第三 (19%)。

在亚太地区的事件中，日本占 91%，菲律宾占 5%，澳大利亚、印度和越南各占 1.5%。

在亚太地区，制造业是受攻击最严重的行业，事件占比达 48%。

## #2 | 欧洲

在欧洲，部署后门攻击从 2022 年 3 月开始激增，时间就发生在俄罗斯入侵乌克兰之后。在该区域的安全事件中，部署后门攻击占 21%，勒索软件占 11%。在 X-Force 响应过的事件中，远程访问工具占 10%。关于对客户的影响，X-Force 在欧洲观察到的事件中有 38% 与勒索有关，17% 导致了数据盗窃，14% 为凭证收集。欧洲是受勒索攻击最严重的区域，在所观察到的所有勒索事件中占比达 44%。

利用面向公众应用程序中出现的漏洞是针对欧洲组织的主要感染媒介，在 X-Force 于该区域补救过的所有事件中占比达 32%，其中有数例直接造成勒索软件感染。滥用有效本地帐户排名第二 (18%)，鱼叉式网络钓鱼链接排名第三，从 2021 年的 42% 大幅下降到 14%。鱼叉式网络钓鱼链接的下降可能是因为用户意识的提高、电子邮件安全防御的加强，或安装了具有更强恶意软件捕捉功能的防御系统。

专业服务、商业和消费者服务业和金融与保险业都是受攻击最严重的行业，在 X-Force 响应过的事件中占比均为 25%。制造业排名第二 (12%)，能源业和医疗保健业都排名第三 (10%)。

英国是欧洲受攻击最严重的国家，事件占比达 43%。德国占 14%，葡萄牙占 9%，意大利占 8%，法国占 7%。X-Force 还在挪威、丹麦、瑞士、奥地利、希腊、格陵兰、西班牙和塞尔维亚响应过较小数量的事件。

英国是欧洲受攻击最严重的国家，事件占比达 43%。

## #3 | 北美

X-Force 观察到北美的事件稍有增加，从 2021 年的 23% 上升到了 2022 年的 25%。

能源公司上升为北美的主要受害者，在 X-Force 2022 年响应过的所有攻击事件中占比达 20%。制造业和零售批发业并列第二名，均占 14%。虽然零售批发业与 2021 年的情况相似，但制造业的事件却比 2021 年下降了 50%。专业服务、商业和消费者服务业在 2022 年排名第三 (12%)，勒索软件和其他恶意软件相关事件有所上升。

识别到的主要感染媒介是利用公众应用中出现的漏洞 (35%) 和鱼叉式网络钓鱼附件 (20%)。勒索软件事件占比达 23%，其中有几例是由于检测到 2018 年或 2019 年感染后未清除的 WannaCry 或 Ryuk，这凸显了在此类事件后进行恰当清除的重要性。在该区域，僵尸网络占安全事件的 12%，后门攻击和 BEC 各占 10%，并列第三名。

在威胁攻击者造成的主要影响方面，凭证收集排名第一，在 X-Force 于北美补救过的事件中占比达 25%。数据泄漏和数据盗窃并列第二名（各占 17%），勒索占第三名 (13%)。

在该区域的攻击中，美国占比达 80%，而加拿大仅为 20%。

北美受攻击最严重的组织是能源公司，事件占比达 20%。

## #4 | 拉丁美洲

出于报告目的，IBM 考虑将墨西哥、中美洲和南美洲计入拉丁美洲。

拉丁美洲的事件与全球趋势相反，其零售批发业是受攻击最严重的行业，在 X-Force 补救过的事件中占比达 28%，从 2021 年的第二名上升了。金融与保险业排名第二 (24%)，然后是能源业 (20%)。

在拉丁美洲，勒索软件攻击超过了其他攻击，在 X-Force 响应过的事件中占比达 32%。部署后门攻击是针对目标采取的第二大行动 (16%)，BEC 和电子邮件线程劫持并列第三名（各占 11%）。勒索和数据盗窃是该区域最常见的影响，事件占比达 27%，经济损失排名第二 (20%)，数据破坏和泄漏并列第三名（各占 13%）。

主要的初始访问媒介包括外部远程服务 (30%) 和利用公众应用中出现的漏洞 (20%)。偷渡式泄露、硬件添加、有效域帐户、有效本地帐户和鱼叉式网络钓鱼附件各占 10%。

在 X-Force 于拉丁美洲响应过的所有事件中，巴西占 67%，哥伦比亚占 17%，墨西哥占 8%。秘鲁和智利共占 8%。

在 X-Force 于拉丁美洲响应过的所有事件中，巴西占 67%。

## #5 | 中东和非洲

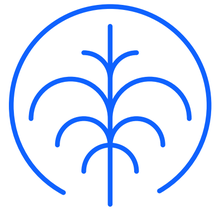
出于报告目的，IBM 考虑将黎凡特、阿拉伯半岛、埃及、伊朗和伊拉克以及整个非洲大陆计入中东和非洲。

在 X-Force 2022 年于该区域响应过的事件中，部署后门占比达 27%。勒索软件和蠕虫都是第二大常见攻击类型，各占 18%。在该区域 2021 年事件的影响方面，勒索和经济损失各占了一半。

在 X-Force 于中东和非洲补救过的事件中，三分之二使用了鱼叉式网络钓鱼链接作为初始访问媒介，另外三分之一则使用了可移动介质。金融和保险业是 2022 年中东和非洲受攻击最严重的行业，事件占比达44%，比 2021 年的 48% 有所下降。专业服务、商业和消费者服务业在攻击事件中占比达 22%，制造业和能源业排名第三，各占 11%。

在 X-Force 于该区域响应过的事件中，沙特阿拉伯占了三分之二。其余事件分布在卡塔尔、阿联酋和南非。

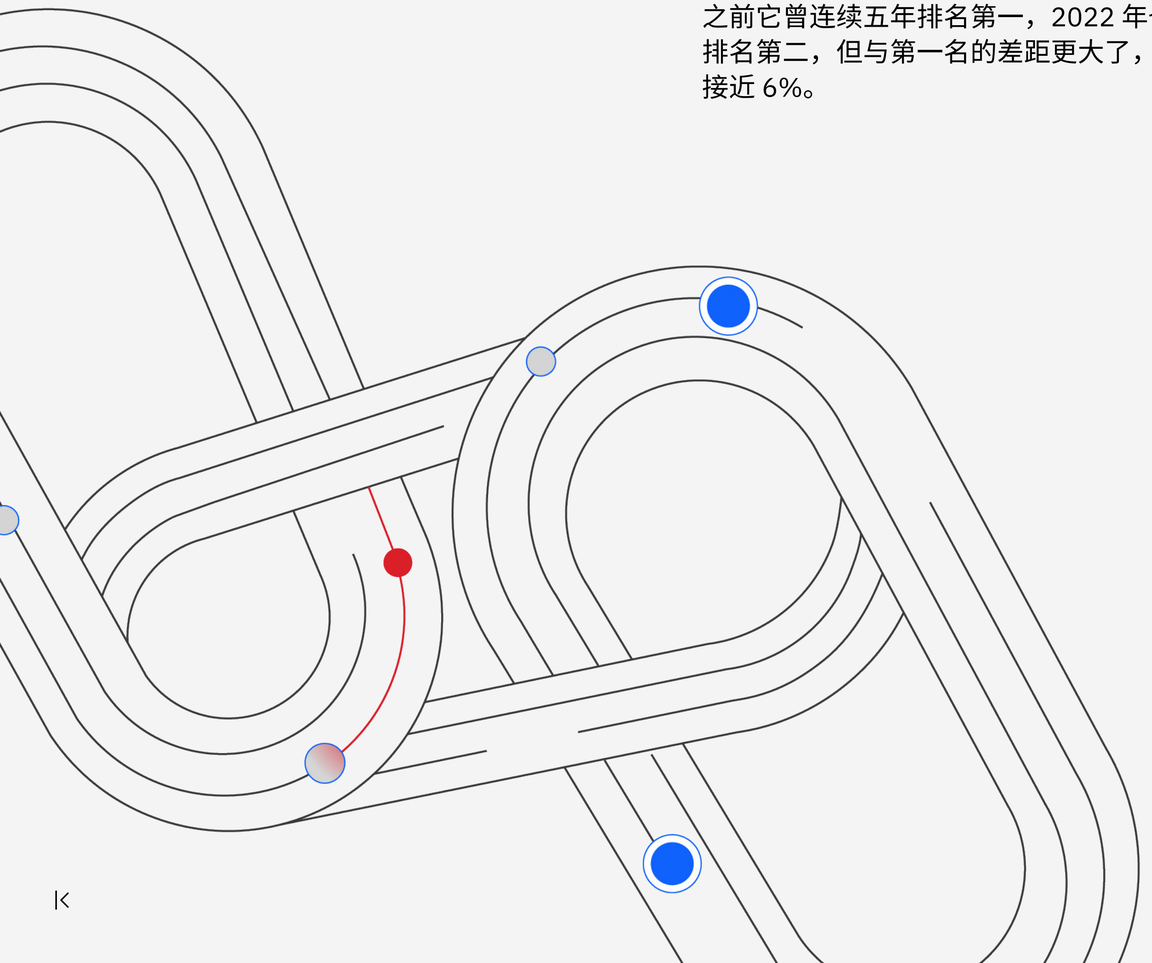
部署后门是此区域最常见的攻击，威胁事件占比高达 27%。



11

# 行业趋势

X-Force 事件响应数据显示，制造业已连续两年成为受攻击最严重的行业。金融与保险业 2021 年仅以 1% 的差距排名第二，在此之前它曾连续五年排名第一，2022 年也是排名第二，但与第一名的差距更大了，接近 6%。



2018 – 2022 年行业攻击占比概况

| 行业 | 2022 年 | 2021 年 | 2020 年 | 2019 年 | 2018 年 |
|---|---|---|---|---|---|
| 制造 | 24.8% | 23.2 | 17.7 | 8 | 10 |
| 金融与保险 | 18.9% | 22.4 | 23 | 17 | 19 |
| 专业服务、商业和消费者服务业 | 14.6% | 12.7 | 8.7 | 10 | 12 |
| 能源 | 10.7% | 8.2 | 11.1 | 6 | 6 |
| 零售批发 | 8.7% | 7.3 | 10.2 | 16 | 11 |
| 教育 | 7.3% | 2.8 | 4 | 8 | 6 |
| 医疗保健 | 5.8% | 5.1 | 6.6 | 3 | 6 |
| 政府 | 4.8% | 2.8 | 7.9 | 8 | 8 |
| 运输 | 3.9% | 4 | 5.1 | 13 | 13 |
| 媒体和电信 | 0.5% | 2.5 | 5.7 | 10 | 8 |

## 24.8%

X-Force 响应过的事件发生在制造业的比例

### #1 | 制造业

制造业是受攻击最严重的行业，所占比例比 2021 年稍高。2022 年，部署后门攻击的威胁事件占比达 28%，超过了勒索软件，后者在 X-Force 补救过的安全事件中占比为 23%。Emotet 感染的爆发也推动了部署后门攻击的高占比。其中一些事件本可导致勒索软件攻击及其他更恶意的活动，但被及早发现并采取了补救措施。

鱼叉式网络钓鱼附件和利用公众应用中出现的漏洞并列感染媒介第一名，各占 28%。外部远程服务排名第二 (14%)，鱼叉式网络钓鱼链接和有效默认帐户并列初始访问媒介第三名（各占 10%)。

勒索是对制造业组织产生的主要影响，事件占比达 32%。众所周知，制造商几乎不能容忍停机，这使勒索成为攻击者的获利策略。数据盗窃是第二常见的攻击，事件占比达 19%，然后是数据泄漏 (16%)。亚太地区发生的制造业事件最多，占比高达 61%。欧洲和北美并列第二名 (14%)，然后是拉丁美洲 (8%) 与中东和非洲 (4%)。

## 18.9%

X-Force 响应过的事件发生在金融与保险业的比例

### #2 | 金融与保险

在 X-Force 2022 年响应过的事件中，金融与保险组织占比不到五分之一，排名第二。这一占比显示该行业在过去几年的受攻击数呈缓慢下降趋势，因为其他行业开始受到攻击者的注意，尤其是制造业。

与其他行业相比，金融与保险组织的数字化转型和云采用进程更快。因此，攻击者可能需要付出更大代价才能成功对这些组织实施攻击。

在所观察到针对目标采取的行动中，后门攻击最常见 (29%)，然后是勒索软件和恶意文件（各占 11%）。鱼叉式网络钓鱼附件是主要感染媒介，在此行业的攻击事件中占比高达 53%。利用公众应用中出现的漏洞排名第二 (18%)，然后是鱼叉式网络钓鱼链接 (12%)。

欧洲受攻击最严重的是金融与保险组织，事件占大约为 33%，亚太地区紧随其后，排名第二 (31%)。在 X-Force 响应过的事件中，拉丁美洲占比约 15%，北美、中东和非洲各占比约 10%。

## 14.6%

X-Force 响应过的事件发生在专业服务、商业和消费者服务业的比例

### #3 | 专业服务、商业和消费者服务业

专业服务业包括咨询公司、管理公司和法律公司。这些服务占此行业受害者的 52%。相反，商业服务则包括 IT 和技术服务、公共关系、广告和传播等公司。这些服务占受害者的 37%。消费者服务包括住宅建筑商、房地产、艺术、娱乐和休闲等，占受害的 11%。这些行业合起来形成了 2023 年 X-Force 威胁情报指数中的专业服务、商业和消费者服务类别。

专业服务行业、商业和消费者服务业受到最多的攻击是勒索软件和后门攻击（各占 18%）。利用公众应用中出现的漏洞和外部远程服务是主要感染媒介（各占 23%）。鱼叉式网络钓鱼附件和有效本地帐户则各占 15%。

勒索是最常见的影响，事件占比达 28%，然后是数据盗窃、凭证收集和数据泄漏（各占 17%）。在 X-Force 响应过的事件中，欧洲占 47%，北美占 33%，亚太地区占 10%，中东和非洲占 7%，拉丁美洲占 3%。

# 10.7%

X-Force 响应过的事件发生在能源行业的比例

## #4 | 能源

能源组织（包括电力公用事业公司和油气公司）是第四大受攻击行业（与 2021 年排名一样），事件占比为 10.7%。利用公众应用中出现的漏洞是最常见的感染媒介，占比达 40%。鱼叉式网络钓鱼链接和外部远程服务则各占 20%。僵尸网络是针对目标采取的主要行动，事件占比达 19%，勒索软件和 BEC 并列第二名（各占 15%）。

数据盗窃和勒索的事件占比达 23%，然后是凭证收集和僵尸网络感染（各占 15%）。在 X-Force 在全球响应过的所有事件中，北美组织是主要受害者 (46%)，然后是欧洲和拉丁美洲（各占 23%），亚太地区、中东和非洲占比则不到 5%。

能源业依然面临来自各种全球各种力量的压力，尤其是因俄乌战争而恶化的势力，及其对原本就已动荡不稳的全球能源贸易的影响。

## 8.7%

X-Force 响应过的事件发生在零售批发业的比例

### #5 | 零售批发业

零售商负责向消费者和批发商出售商品。批发商一般负责将来自制造商的这些商品直接运输和分销给零售商或消费者。X-Force IR 数据显示，零售批发业是第五大受攻击行业（与 2021 年排名一样）。

在零售批发业的攻击事件中，主要初始访问媒介是含有恶意链接的鱼叉式网络钓鱼电子邮件，占比达 33%。遭到入侵的外部远程服务、含有恶意附件的鱼叉式网络钓鱼和硬件添加各占 17%。

勒索软件、后门入侵和 BEC 是攻击者采取的主要行动，各占 19%； 蠕虫占 10%。在受害者经历的事件影响中，勒索占 50%，凭证收集和经济损失各占 25%。受攻击最严重的地区是北美和拉丁美洲（各占 39%），然后是欧洲 (22%)。

# 7.3%

X-Force 响应过的事件发生在教育业的比例

## #6 | 教育业

在 X-Force 响应过的教育业攻击事件中，后门占比 20%；勒索软件、广告软件和垃圾邮件各占 13%。利用公众应用中出现的漏洞是观察到的主要初始访问媒介，事件占比达 42%，然后是鱼叉式网络钓鱼附件 (25%)。通过服务和链接进行的网络钓鱼，以及有效云和本地帐户滥用则各占 8%。在事件影响方面，数据盗窃、数据泄漏、勒索和侦察各占 25%。亚太地区的事件占比达 67%，然后是北美 (27%) 和拉丁美洲 (6%)。

# 5.8%

X-Force 响应过的事件发生在医疗保健业的比例

## #7 | 医疗保健

在前十大行业中，医疗保健业回落到第七名，比 2021 年的第六名又进一步下降。
在 X-Force 响应过的事件中，医疗保健业的占比在过去三年都维持在大约 5%-6%。
后门攻击的事件占比为 27%，脚本木马占比为 18%。广告软件、BEC、加密挖掘器、载入程序、侦察和扫描工具和远程访问工具各占 9%。在观察到的事件影响中，侦察占高达 50%，数据盗窃和数字货币挖掘则各占 25%。

基于欧洲的目标占事件的 58%，北美目标占 42%。

# 4.8%

X-Force 响应过的事件发生在政府部门的比例

## #8 | 政府

政府实体是后门攻击的另一个主要目标，在 X-Force 事件响应 (IR) 案例中占比达 25%。DDoS 攻击的事件占比也是 25%。公共部门网络中的大量敏感信息是网络间谍活动的常见目标之一。此信息包括巨大的 PII 数据库，以及可能被国家支持的团伙使用或网络罪犯出售获利的其他信息。恶意文件 (Maldoc) 的事件占比为 17%，加密挖掘器、凭证获取工具、勒索软件和脚本木马总占比为 83%。

对于此领域的事件，X-Force 可将事件与网络罪犯、导致数据破坏的内部威胁、黑客行为主义者以及在国家支持下从事间谍活动的威胁团伙关联，这些事件的占比相等。

利用公众应用中出现的漏洞和鱼叉式网络钓鱼附件是主要感染媒介，各占 40%；滥用有效默认帐户占 20%。亚太地区的政府实体是主要攻击目标，事件占比高达 50%，然后是欧洲 (30%) 和北美 (20%)。

## 3.9%

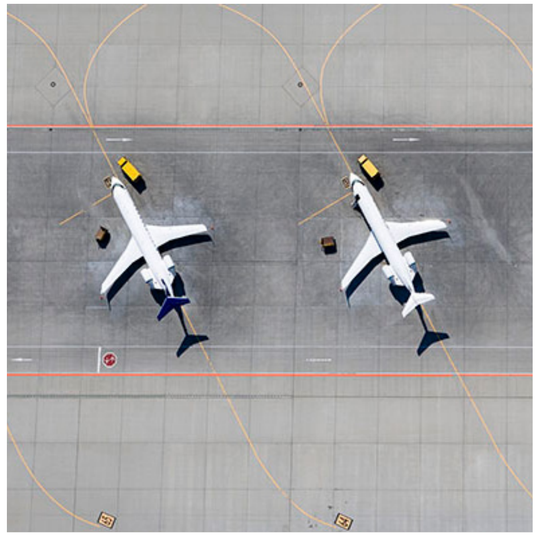
X-Force 响应过的事件发生在运输业的比例

### #9 | 运输业

运输业在 2021 年排名第七，2022 年回到了它在 2020 年的第九位排名。但是，该行业在 X-Force 响应过的事件中的占比大致不变。网络钓鱼是最常见的初始访问媒介，事件占比达 51%，其中链接、附件和服务伪装鱼叉式网络钓鱼占比相同。滥用有效本地帐户作为主要访问媒介的占比为 33%，有效云帐户作为入口点的占比为 17%。

针对目标采取的首要行动是服务器访问和部署远程访问工具（各占 25%），然后是垃圾邮件活动、勒索软件、后门和篡改（各占 13%）。

数据盗窃是最常见的影响，事件占比达 50%，勒索和对品牌声誉的影响各占 25%。欧洲的运输实体受攻击最严重，事件占比达 62%，亚太地区排名第二，刚超过 37%。



# 0.5%

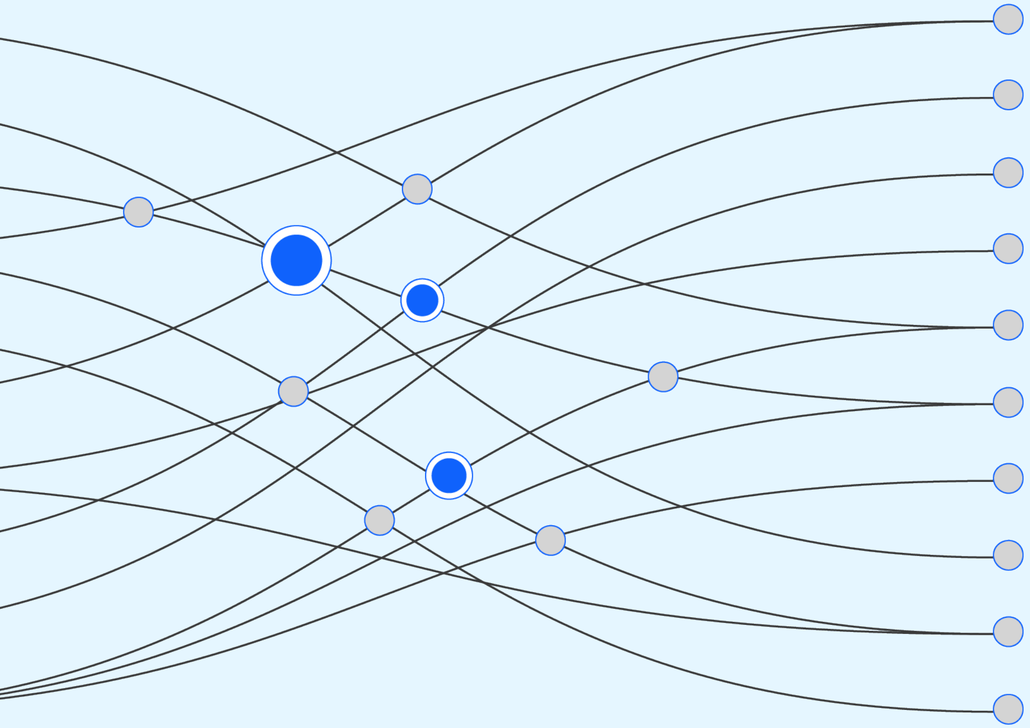
X-Force 响应过的事件发生在媒体和电信业的比例

## #10 | 媒体和电信业

在 X-Force 响应过的事件中，媒体和电信占比很小，已连续两年排名最后。滥用外部远程服务（例如 VPN 和其他访问机制）和有效域帐户是观察到的感染媒介。这些媒介导致了勒索软件攻击。在这些事件中观察到的行动包括部署勒索软件和数据渗漏工具。
这些行动反过来又导致了数据盗窃、泄漏、破坏和勒索等活动。

12

# 建议



以下行动建议有助于保护贵组织不受恶意威胁侵害，包括此报告中所述的威胁。

**管理您的资产：**“我们有什么？我们在保护什么？什么数据对我们的业务至关重要?”要构建成功的防御，任何安全团队都应先回答这些问题。优先安排发现组织外围的资产、了解组织的网络钓鱼攻击隐患并减少那些攻击面能进一步提升整体安全性。最后，组织必须扩展其资产管理计划，以纳入源代码、凭证和其他可能已经存在于互联网或暗网中的数据。

**了解您的对手：**虽然许多组织拥有威胁发展态势的广泛视图，但是 X-Force 建议组织用突出显示最有可能以您的行业、组织和地理位置为目标的具体威胁参与者的视图。该视图包括了解威胁参与者如何运作、确定其复杂度，以及了解攻击者最有可能使用的策略、技巧和程序。

**管理可见性：**在深入了解最有可能攻击组织的对手之后，组织必须确认拥有能发现攻击者入侵数据源的适当可见性。保持整个组织关键点的可视化管理，确保能及时生成警报及采取相应行动，对于在攻击者造成破坏之前就阻止他们至关重要。

**挑战假设：**组织必须假设其已被入侵。这样，团队便能继续复查以下内容：

- 攻击者能如何渗透其系统
- 组织对新兴策略、技巧和程序的检测和响应能力如何
- 潜在对手入侵组织最关键的数据和系统的难度

最成功的安全团队会定期执行攻击测试，包括威胁追踪、渗透测试和基于目标的红队组队，以检测或验证伺机入侵其环境的攻击路径。

**根据情报采取行动：**在所有位置应用威胁情报。有效的威胁情报应用除了帮助发展高度精确的检测机会之外，还可让您分析常见的攻击路径和识别减轻常见攻击的关键机会。在应用威胁情报的同时，应了解您的对手及其如何运作。

**做好准备：**攻击不可避免，但失败可以避免。组织应根据其环境定制事件响应计划。随着组织发生改变，应以改进响应、补救和恢复时间为中心，定期演练和修改这些计划。

采用信誉良好的 IR 供应商，可以减少熟练的响应者用于缓解攻击所需的专门时间。另外，在制定和测试响应计划时纳入 IR 供应商至关重要，有助于提升相应的效果和效率。最优化的 IR 计划会包含跨组织的响应，纳入 IT 之外的利益相关者，以及测试技术团队和高层领导之间的沟通渠道。最后，在沉浸式高压网络靶场演练中测试计划，能够大幅提升组织响应攻击的能力。

通过这些行动提高安全性：

- [ ] 管理您的资产
- [ ] 了解您的对手
- [ ] 管理可见性
- [ ] 挑战假设
- [ ] 根据情报采取行动
- [ ] 做好准备

# 关于我们

## IBM Security X-Force

IBM Security X-Force 是一个专注威胁处理的团队，由黑客、响应者、研究人员和分析师组成。X-Force 的产品组合包括各种进攻型和防御型产品和服务，采用 360 度威胁视图开展运营和管理。

在网络攻击肆虐横行、万物互联和监管要求越来越严的时代，组织需要采取一种目标明确的安全方法。X-Force 认为，我们应重点关注威胁。通过渗透测试、漏洞管理和对手模拟服务，X-Force Red 团队的黑客扮演威胁实施者，寻找可能暴露最重要资产的安全漏洞。通过事件准备、检测和响应，以及危机管理服务，X-Force 事件响应团队对威胁的藏身之处以及阻止其造成侵害的方法了然于胸。X-Force 研究人员开发进攻性的威胁检测和预防技术，而 X-Force 分析人员可以收集威胁数据并将其转化为用于降低风险的可用信息。

X-Force 深入了解威胁实施者的思维方式、策略和攻击方式，可以帮助您预防、检测、应对事件和从事件中恢复，确保您专注于优先级更高的业务活动。

如果您的组织希望在强化云安全态势方面获取支持，请预约 IBM Security X-Force 专家进行一对一咨询。

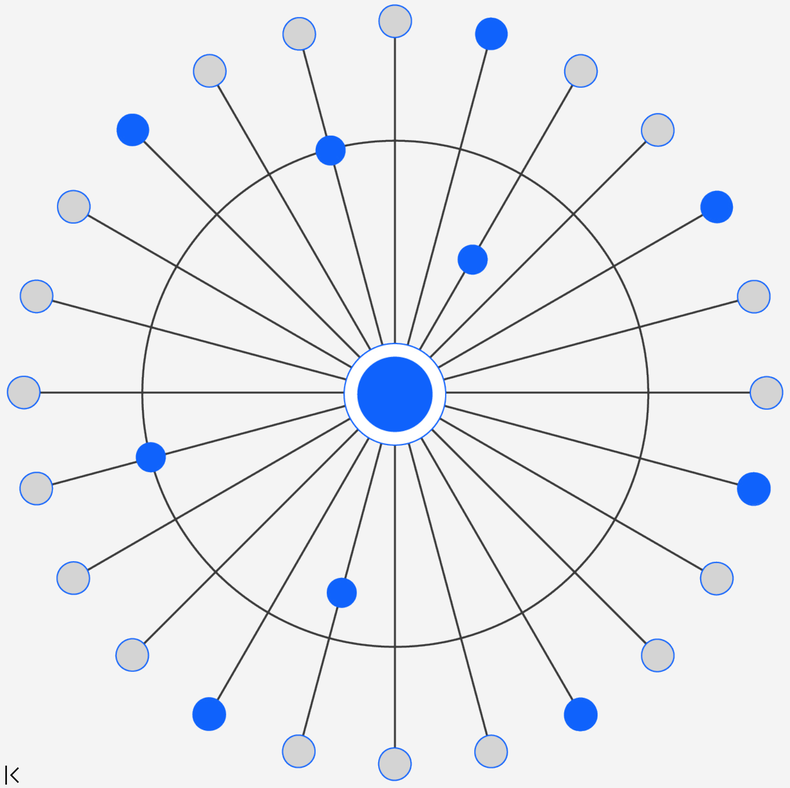
预约咨询 →

## IBM Security

IBM Security 根据您不断扩展的覆盖范围，密切契合需求，与您携手保护组织安全环境。我们利用动态 AI 和自动化功能，帮助您确保始终领先一步，实现更快的速度和更高的准确性。我们行业领先的专家组成的团队值得信赖，全程为您提供洞察分析，助您始终采取正确的行动，让您安心无忧。从预测威胁到帮助保护数据； 工作范围涵括所有供应商且覆盖全球各地； 无论您的业务方向如何，IBM Security 都能助您实现宏伟的业务目标，同时探索关键的新技术并帮助尽量减少意外的威胁。

了解更多信息 →

# 报告撰稿人名录



Michael Worley
Christopher Caridi
Michelle Alvarez
Karlina Bakken
Yannick Bedard
Michele Brancati
Christopher Bedell
Joshua Chung
Scott Craig
Joseph DiRe
John Dwyer
Emmy Ebanks
Richard Emerson
Charlotte Hammond
Kevin Henson
Guy-Vincent Jourdan
Vio Onut
Mitch Mayne
Dave McMillen
Kat Metrick
Scott Moore
Golo Mühr
Andy Piazza
Benjamin Shipley
Christopher Thompson
Ole Villadsen
Reginald Wong
John Zorabedian

# 15

# 附录

## 影响列表

| 影响 | 影响 |
| --- | --- |
| 僵尸网络 | 数字货币挖掘 |
| 品牌声誉 | 间谍 |
| 凭证收集 | 勒索 |
| 数据破坏 | 经济损失 |
| 数据泄漏 | 生产中断 (OT) |
| 数据盗窃 | 侦察 |

1. “A timeline of the biggest ransomware attacks”，CNET，2021 年 11 月 15 日
2. “International action against DD4BC cybercriminal group”，Europol，2016 年 1 月 12 日
3. “DD4BC, Armada Collective, and the Rise of Cyber Extortion”，Recorded Future，2015 年 12 月 7 日
4. “A Brief History of Ransomware”，Varonis，2015 年 11 月 10 日
5. “Inside Chimera Ransomware - the first ‘doxingware’ in wild”，MalwardBytes Labs，2015 年 12 月 8 日
6. “Big Game Hunting: The Evolution of INDRIK SPIDER From Dridex Wire Fraud to BitPaymer Targeted Ransomware”，Crowdstrike，2018 年 11 月 14 日
7. “Operators of SamSam Continue to Receive Significant Ransom Payments”，Crowdstrike，2018 年 4 月 11 日
8. “Triple Extortion Ransomware: The DDoS Flavour”，PacketLabs，2022 年 5 月 12 日
9. “They Told Their Therapists Everything. Hackers Leaked It All”，Wired，2021 年 5 月 4 日
10. “BazarCall to Conti Ransomware via Trickbot and Cobalt Strike”，The DFIR Report，2021 年 8 月 1 日
11. “Diavol Ransomware”，The DFIR Report，2021 年 12 月 13 日
12. “Quantum Ransomware”，The DFIR Report，2022 年 4 月 25 日
13. “Bumblebee Loader Linked to Conti and Used In Quantum Locker Attacks”，Kroll，2022 年 6 月 6 日
14. “This isn’t Optimus Prime’s Bumblebee but it’s Still Transforming”，Proofpoint，2022 年 4 月 28 日
15. “Understanding REvil: REvil Threat Actors May Have Returned (Updated)”，Unit 42，2022 年 6 月 3 日
16. “AdvIntel’s State of Emotet aka “SpmTools” Displays Over Million Compromised Machines Through 2022,” AdvIntel，2022 年 9 月 13 日
17. “Back in Black: Unlocking a LockBit 3.0 Ransomware Attack,” NCC Group，2022 年 8 月 19 日
18. “Back in Black: Unlocking a LockBit 3.0 Ransomware Attack,” NCC Group，2022 年 8 月 19 日





国际商业机器（中国）有限公司
了解更多信息，欢迎访问我们的中文官网：
**https://www.ibm.com/cn-zh**

美国出品
2023 年 2 月