IBM **Security**

X-Force 威胁情报指数 2022

IBM

目录

执行摘要

疫情仍在肆虐，整个世界继续苦苦挣扎；企业和组织在居家工作和返岗复工之间来回摇摆；地缘政治的变化催生了持续的不信任。这一切都造成了混乱不堪的局面，而网络犯罪分子则有了可乘之机。在 2021 年，IBM Security® X-Force® 看到了威胁实施者如何抓住机会，利用不断变化的局面，采用各种手段和方法，成功渗透进世界各地的组织中。

IBM Security X-Force 威胁情报指数总结了我们从数据中发现和分析出的新趋势和攻击模式，这些数据是从数十亿个数据点收集的，包括终端检测设备、事件响应 (IR) 互动和域名跟踪等。本报告是基于从 2021 年 1 月至 12 月收集的数据的研究结论。

我们将这些研究成果作为一种资源，提供给 IBM 客户、安全行业的研究人员、政策制定者、媒体以及更广泛的安全专业人士和业务领导群体。

鉴于业务格局变幻不定，威胁类型和威胁方向不断发展，您比以往任何时候都更需要掌握深入的威胁情报洞察，抢在攻击者之前占得先机，强化关键资产的安全性。

报告要点

最主要的攻击类型：勒索软件再次占据 2021 年最主要攻击类型的榜首，尽管在 X-Force 修复的攻击中，勒索软件的百分比同比下降了近 9%。REvil（一种勒索软件类型，X-Force 也将其称为 Sodinokibi）是 X-Force 连续第二年观察到的最常见的勒索软件类型，占全部勒索软件攻击的 37%，而排在第二位的 Ryuk 占比只有 13%。2021 年勒索软件和物联网僵尸网络攻击之所以有所减少，执法活动可能是主要原因，但这并不能排除这些攻击在 2022 年死灰复燃的可能性。

供应链漏洞：供应链安全性受到了政府和政策制定者的重点关注，拜登政府关于网络安全的总统行政令以及美国国土安全部、CISA 和 NIST 的指南都强调了零信任。这些准则聚焦于安全漏洞和可信关系。目前，制造业饱受中断和延迟之苦，雪上加霜的是，该行业也是漏洞利用攻击的重灾区，是犯罪分子初始攻击方向的首选。

钓鱼攻击中使用最多的品牌：X-Force 在整个 2021 年密切跟踪网络犯罪分子如何使用网络钓鱼工具包，我们的研究显示，Microsoft、Apple 和 Google 是犯罪分子尝试假扮的前三大品牌。这些大品牌在网络钓鱼工具包中被反复使用，攻击者利用其热门程度，诱导消费者相信自己。

最主要的威胁团体：疑似的有伊朗国家背景的威胁实施者 ITG17 (MuddyWater)、网络犯罪团体 ITG23 (Trickbot) 和 Hive0109 (LemonDuck) 是 X-Force 情报分析人员在 2021 年观察到的一些最活跃的威胁团体。世界各地的威胁团体都在试图扩充自己的实力，渗透进更多的组织。他们使用的恶意软件嵌入了更狡猾的防御规避方法，在某些情况下，这些恶意软件通过基于云的消息传递平台和存储平台进行托管，以逃过安全控制。恶意软件滥用这些平台，在合法的网络流量中隐藏命令和控制通信。威胁实施者还继续开发 Linux 版本的恶意软件，旨在更轻松地入侵云环境。

主要统计数据：

21%

勒索软件的攻击份额

勒索软件是 X-Force 去年观察到的数量最多的攻击类型，但占比从前年的 23% 下降到去年的 21%。REvil 勒索软件攻击者（又名 Sodinokibi）要为 37% 的勒索软件攻击负责。

17 个月

勒索软件团体改头换面或偃旗息鼓之前的平均生存时间

X-Force 研究的勒索软件团体在改头换面或偃旗息鼓之前的平均生存期为 17 个月。REvil 是最成功的团体之一，在存在 31 个月（两年半）之后于 2021 年 10 月解散。

41%

利用网络钓鱼获得初始访问权限的攻击的百分比

在 2021 年，网络钓鱼行动成为最主要的入侵途径，在 X-Force 修复的安全事件中，有 41% 是通过这种方法获得初始访问权限的。

33%

2020 年至 2021 年间由漏洞利用攻击导致的安全事件数量有所增加

在 2021 年，被犯罪分子利用的五个最主要漏洞中，有四个是新漏洞，包括 Log4j 漏洞 CVE-2021-44228 - 尽管它在 12 月份才被披露，但排名已跃至第二位。

3 倍

增加了电话通话功能的针对性网络钓鱼攻击活动的点击有效性明显提高

有针对性的网络钓鱼活动的平均点击率为 17.8%，但增加了电话通话的针对性网络钓鱼攻击活动（语音钓鱼或语音网络钓鱼）的有效性则提高了三倍，诱使 53.2% 的受害者进行点击。

146%

使用新代码的 Linux 勒索软件显著增加

根据 Intezer 的研究，使用独特（新）代码的 Linux 勒索软件的数量同比增长 146%，这表明 Linux 勒索软件的创新水平显著提升。

#1

制造业受到最多的攻击

制造业取代金融服务业，成为 2021 年受攻击最多的行业，占 X-Force 去年修复的攻击数量的 23.2%。勒索软件是最主要的攻击类型，占到制造企业受到的攻击总数的 23%。

61%

OT 连接的组织在制造业受到的攻击中所占的比例

去年，在制造业中，OT 连接的组织发生的安全事件占总数的 61%。此外，在针对 OT 连接的组织的攻击中，有 36% 是勒索软件。

2,204%

针对 OT 的侦察活动大幅增加

在 2021 年 1 月至 2021 年 9 月期间，攻击者通过互联网针对 SCADA Modbus OT 设备的侦察活动增加了 2,204%。

74%

来自 Mozi 僵尸网络的 IoT 攻击的比例

2021 年，在针对物联网设备的攻击中，源自 Mozi 僵尸网络的攻击占到 74%。

26%

全球攻击中针对亚洲的比例

在所有攻击中，有 26% 以亚洲为目标。亚洲是 2021 年受攻击最多的地理区域。

最主要的攻击类型

在本报告中，我们根据攻击者在获得对受害者网络的访问权限后寻求实现的*最终目标*对攻击类型进行分类。攻击类型与初始感染媒介不同，后者是最初进入网络的方法。

例如，一些攻击类型包括勒索软件、数据盗窃和 BEC，具体取决于威胁发起者操作的最终目标。初始感染媒介的例子包括网络钓鱼、使用被盗凭证和漏洞利用。

以下部分介绍了我们的数据在 2021 年揭示的最多产攻击类型的详细信息和数据。

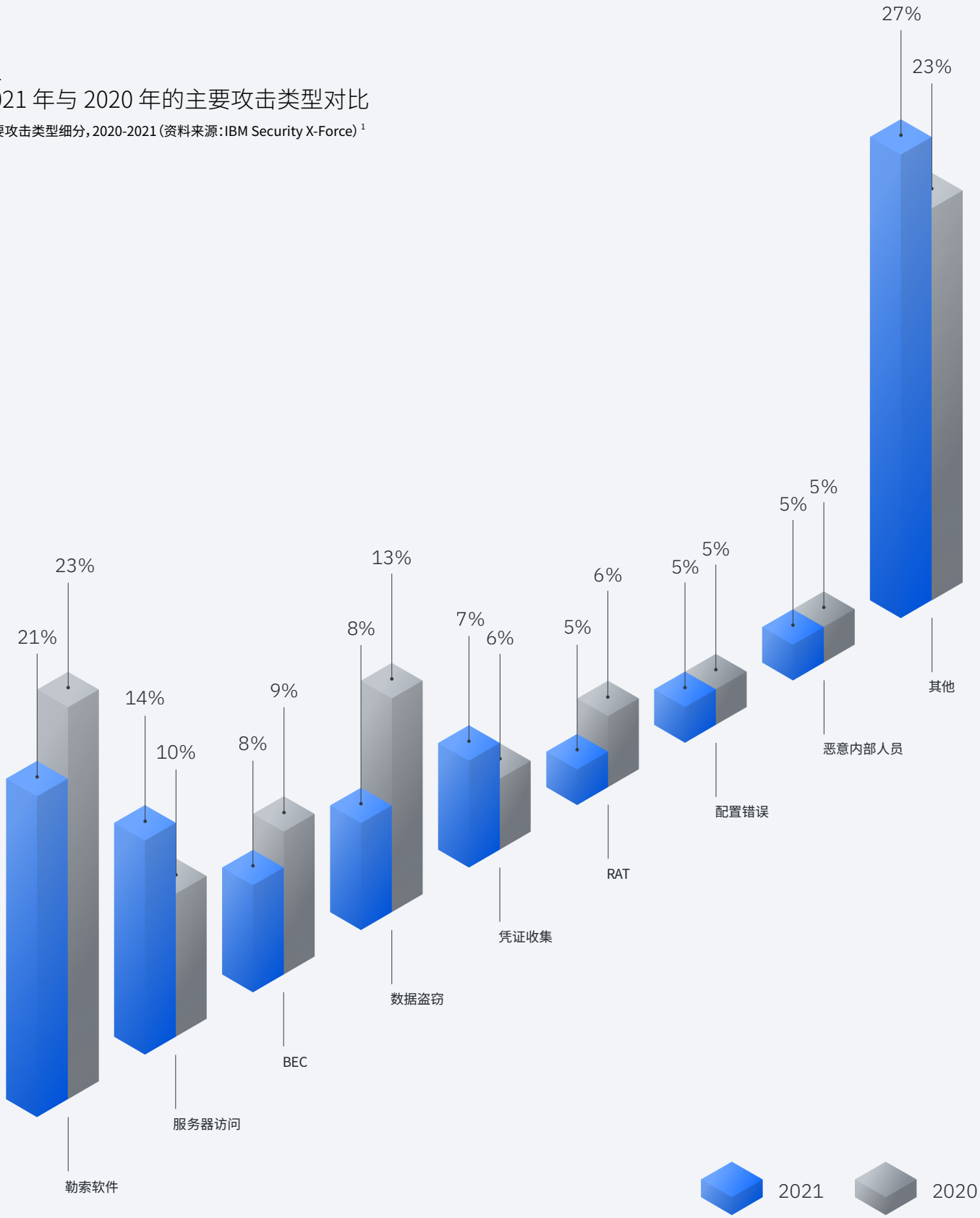
勒索软件

根据 X-Force 的观察，三年多来，勒索软件一直占据主要攻击类型的榜首，2021 年也不例外。X-Force 事件响应团队在 2021 年修复的攻击中有 21% 是勒索软件攻击。这比上一年略有下降，当时 X-Force 团队修复的攻击中有 23% 是勒索软件攻击；但是，勒索软件攻击的数量同比保持稳定。

图 1

2021 年与 2020 年的主要攻击类型对比

主要攻击类型细分，2020-2021（资料来源：IBM Security X-Force）[1]



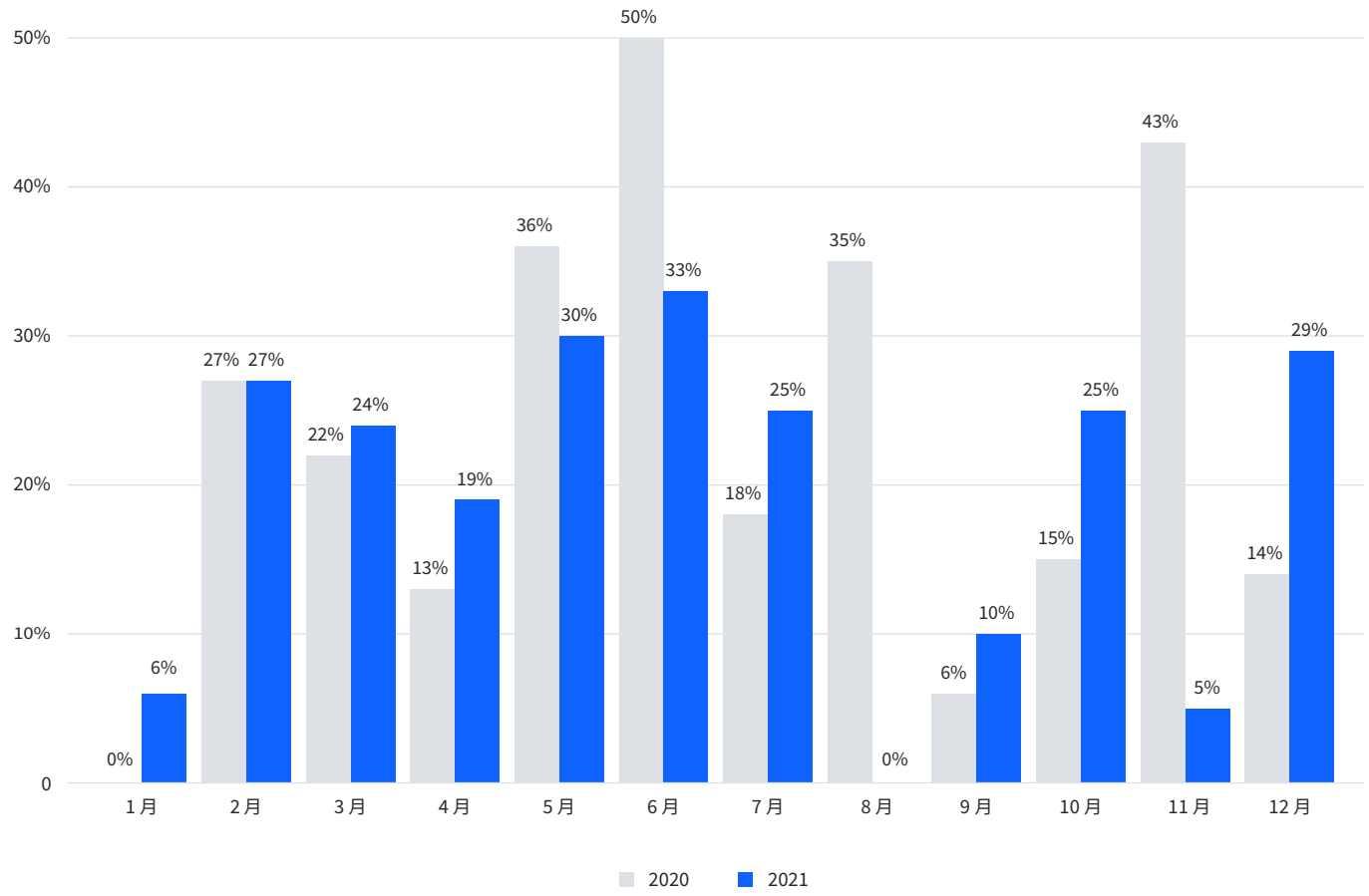
[1]其他攻击包括广告软件、银行木马、僵尸网络、加密矿工、污损、欺诈、DDoS、销售点恶意软件、垃圾邮件、Web 脚本、webshell 和蠕虫。

X-Force 所观察到的勒索软件攻击频率全年都有所变化，其中 5 月和 6 月的攻击频率往往较高，而 1 月的攻击频率则有所降低。此外，勒索软件攻击似乎在夏末或秋初有所减少。在 2021 年，这种下降趋势主要发生在 8 月和 10 月，这可能是由于前几个月若干团伙的永久或暂时性关停：DarkSide 和 Babuk 在 5 月关停运营，Avaddon 在 6 月，而 REvil 则是在 10 月。

图 2

2020 年与 2021 年按月划分的勒索软件攻击占 IR 事件的百分比

勒索软件攻击占 X-Force 事件响应团队所处理攻击的百分比，2020-2021（资料来源：IBM Security X-Force）



根据 X-Force 的研究显示，17 个月是勒索软件团伙更名或关停的平均时间，中位数则为 18 个月。勒索软件团伙不断涌现，而一旦面临被执法部门逮捕或查处的威胁，他们通常就会更名。在某些情况下，执法部门的查处会迫使勒索软件团伙完全关停。尽管这一环境不断变化（或者可能正因为如此），许多勒索软件实施者仍然逍遥法外，基于这种活动所产生的高额利润和目前执法部门在广泛打击勒索软件活动上受到的限制，X-Force 估计，在可预见的未来，犯罪分子的勒索软件活动仍将继续。X-Force 意识到许多勒索软件实施者都已经更名，以新名称继续运营，例如，GandCrab 更名为 REvil、Maze 更名为 Egregor，以及 DoppelPaymer 更名为 Grief。

执法活动可能是降低 X-Force 在 2021 年观察到的勒索软件攻击所占比例的主要因素，但那些已消失的团伙很可能会更名，并在 2022 年以新名称卷土重来，这种勒索软件活动因而也仍将继续。

“许多勒索软件实施者都以新名称继续运营”

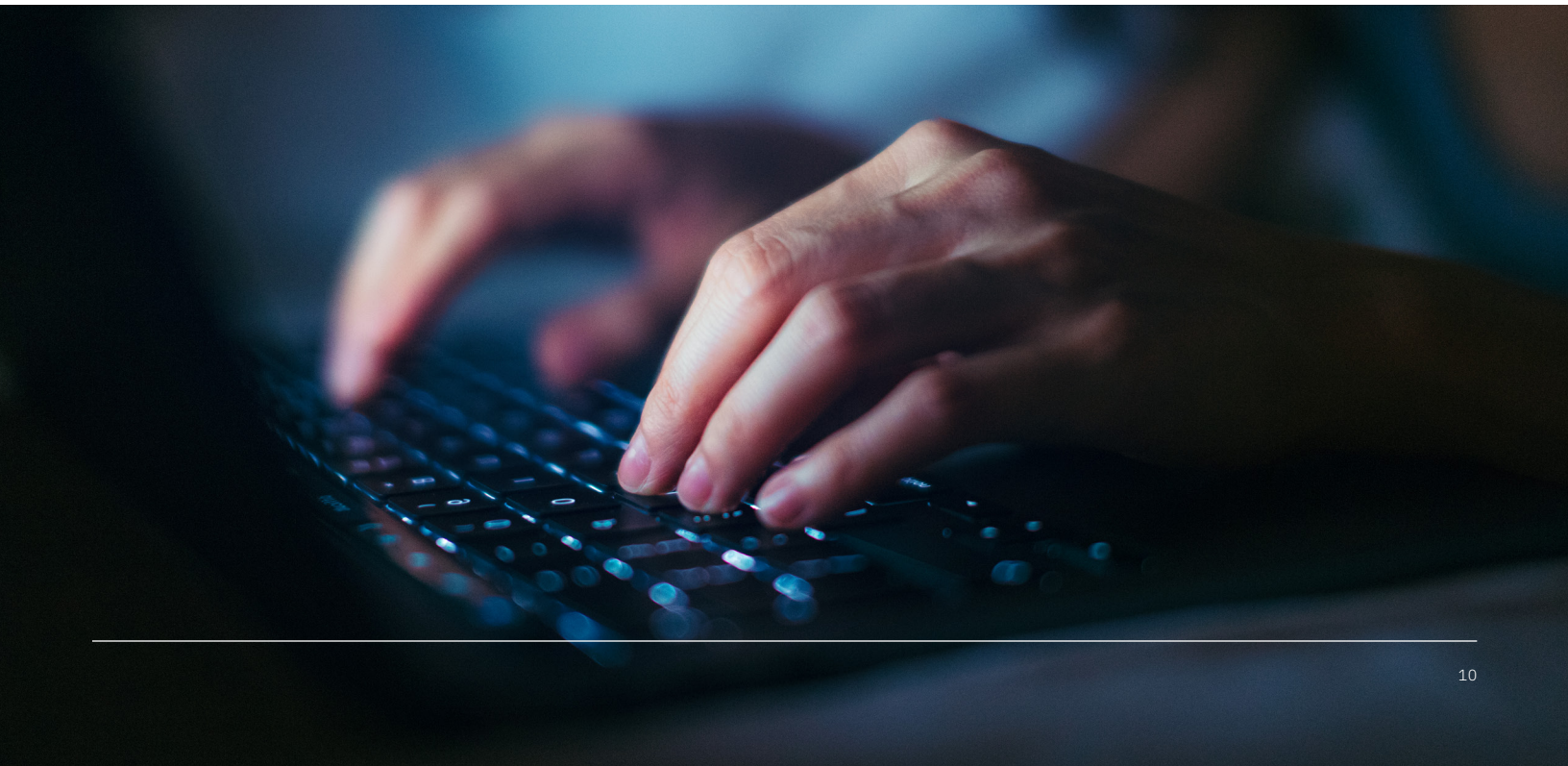
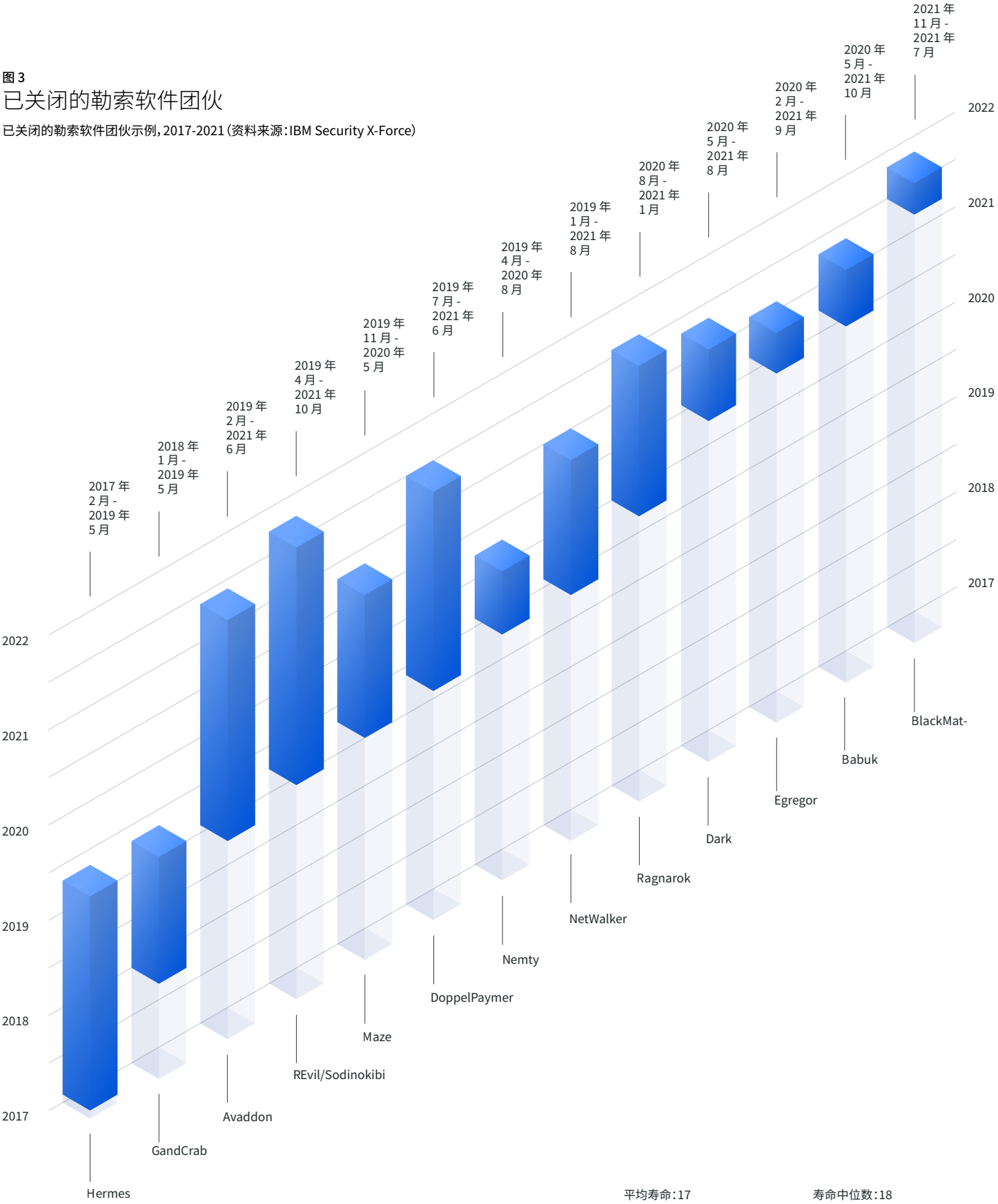


图 3

已关闭的勒索软件团伙

已关闭的勒索软件团伙示例，2017-2021（资料来源：IBM Security X-Force）

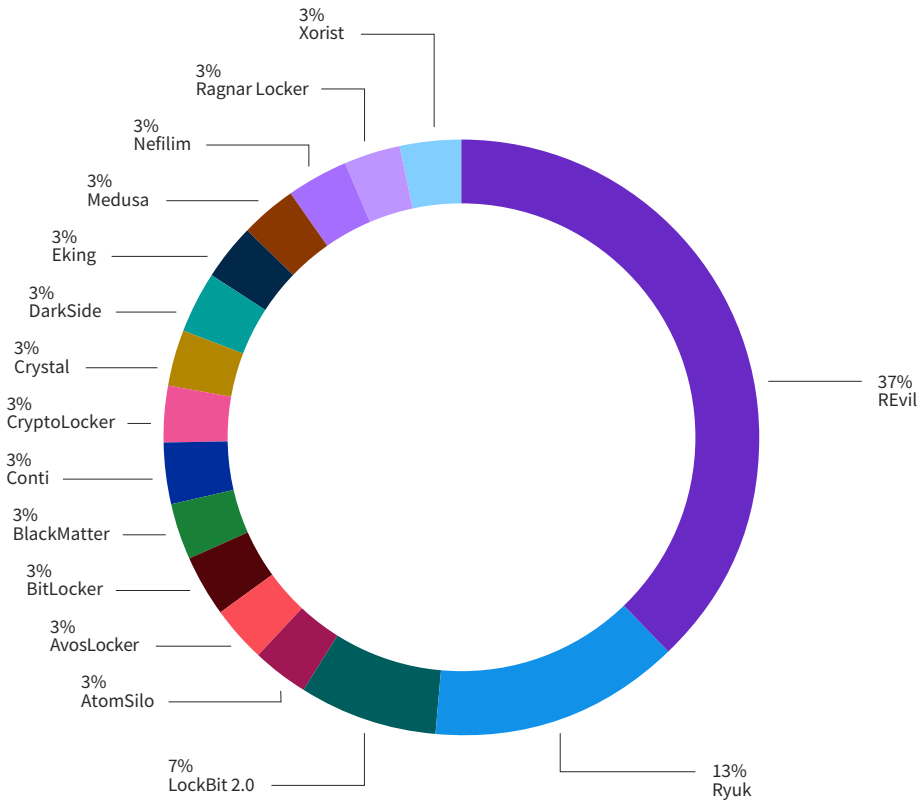


在 X-Force 于 2021 年观察到的勒索软件攻击中，REvil 在我们团队所修复的全部勒索软件事件中占到了 37%（超过三分之一）。Ryuk 则稳居第二位，在去年所观察到的攻击事件中占到了 13%。截至 2021 年 10 月中旬，可能是由于执法活动，REvil 实施者似乎已永久关停运营。Ryuk 和 REvil 分别出现于 2019 年 4 月和 2018 年 8 月，它们都构成了一些运行时间最长的勒索软件活动。

图 4

2021 年观察到的勒索软件类型

X-Force 事件响应团队在 2021 年观察到的勒索软件类型（资料来源：IBM Security X-Force）



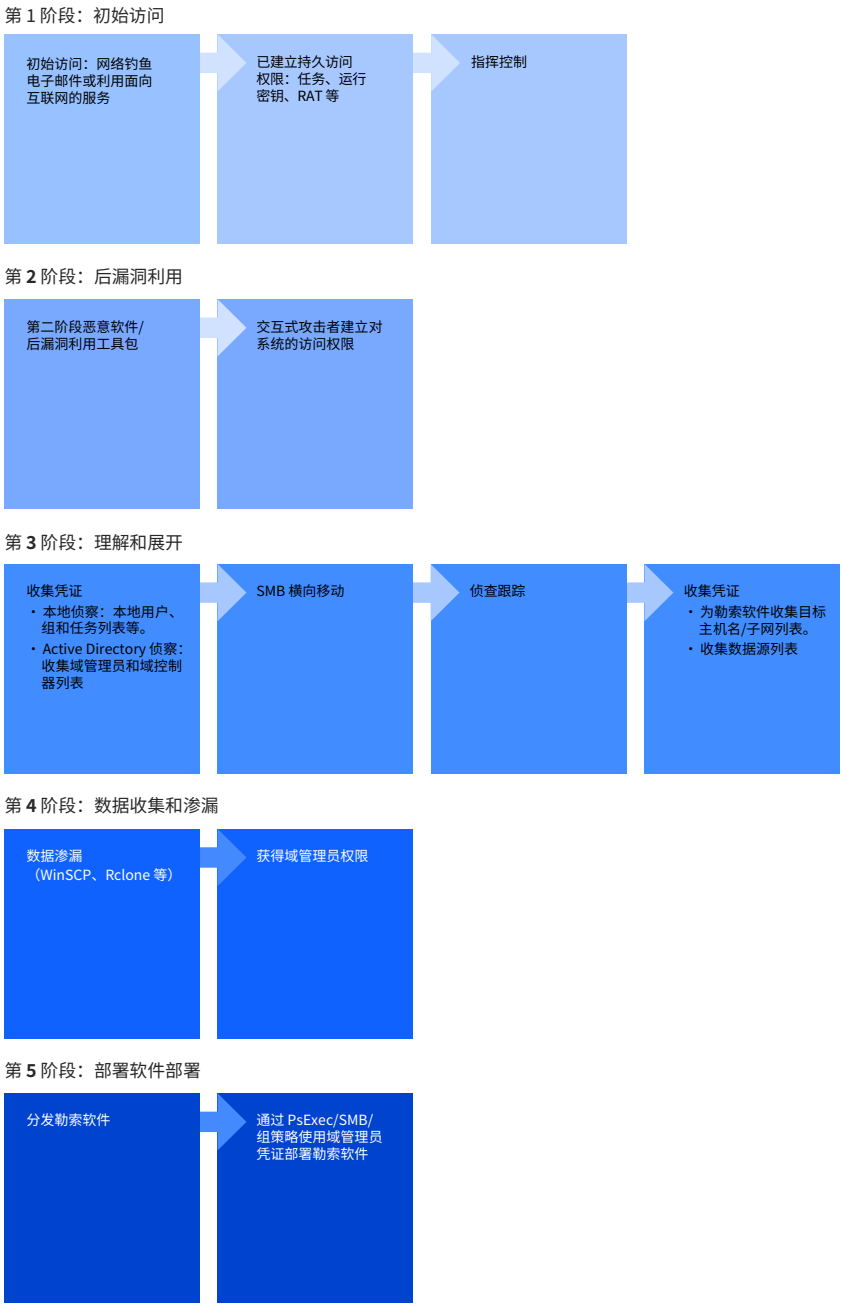
勒索软件如何发起攻击

鉴于 X-Force 事件响应 (X-Force IR) 团队在修复勒索软件攻击方面的丰富经验，我们的团队观察到最近在绝大多数勒索软件攻击中出现的一种模式。尤其是，我们已经能够开发一个五阶段模型，用来定义在大多数勒索软件事件中观察到的常见模式。

图 5

勒索软件攻击的阶段

X-Force 事件响应团队观察到的勒索软件攻击的标准攻击流程（资料来源：IBM Security X-Force）



第 1 阶段：初始访问

勒索软件攻击最常见的访问媒介仍然是网络钓鱼、漏洞利用和远程服务，例如远程桌面协议。

第 2 阶段：后漏洞利用

根据初始访问媒介，第二阶段可能涉及中间远程访问工具 (RAT) 或恶意软件，然后使用攻击性安全工具（例如 Cobalt Strike 或 Metasploit）建立交互式访问。

第 3 阶段：理解和展开

在攻击的第三阶段，攻击者一直专注于理解他们当前可以访问的本地系统和域，并获取额外的凭证来实现横向移动。

第 4 阶段：数据收集和渗漏

自 2019 年以来，X-Force IR 团队响应的勒索软件事件几乎都涉及数据盗窃和勒索软件的“双重勒索”策略。在攻击的第 4 阶段，勒索软件运营商的重点主要转向识别有价值的数据并将其渗漏出来。

第 5 阶段：部署软件部署

在 X-Force IR 团队响应的几乎每一个勒索软件事件中，勒索软件运营商都锁定了域控制器，将其作为勒索软件有效负载的分发点。

勒索软件的一个令人担忧的新趋势就是“三重勒索”策略的扩展。在这种类型的攻击中，威胁实施者不仅加密并窃取数据，还威胁要对受影响的组织发起分布式拒绝服务 (DDoS) 攻击。这种攻击令组织尤为头痛，因为受害者的网络通常会同时被两种恶意攻击所劫持，而数据失窃（通常会造成数据泄露）则会进一步加重其受害程度。

勒索软件团伙开始盯上主要受害者的拓展业务合作伙伴，迫使他们支付赎金，以此来防止因勒索软件攻击而造成的数据泄露或业务中断。

11%

的攻击是服务器访问

服务器访问

服务器访问攻击——攻击者获得对服务器的未经授权的访问，但最终目标未知——是第二常见的攻击类型，在 X-Force IR 团队于 2021 年修复的所有事件中占到了 11%。

这些攻击大多发生在亚洲，在许多情况下，威胁实施者都在服务器上成功地部署了恶意软件或使用渗透测试工具，包括 China Chopper Webshells、Black Orifice 恶意软件、Printspoofer 和 Mimikatz。

在一些情况下，威胁实施者还利用了一个已知漏洞，例如 CVE-2020-7961，这将允许在服务器上远程执行代码。在多种情况下，威胁实施者利用 Microsoft Exchange 服务器中的漏洞，以未经授权的方式访问感兴趣的网络。这些漏洞包含在下面列出的 2021 年十大漏洞中。

在 X-Force 的 IR 团队所观察的服务器访问攻击中，一些攻击虽企图窃取数据或部署勒索软件但却以失败而告终。因此，虽然公司旨在防止攻击者对其网络获得任何级别未经授权的访问，但大量的服务器访问攻击可能表明组织正在积极识别并消除攻击，防止他们进一步发起更具破坏性的操作。

商务电子邮件泄露

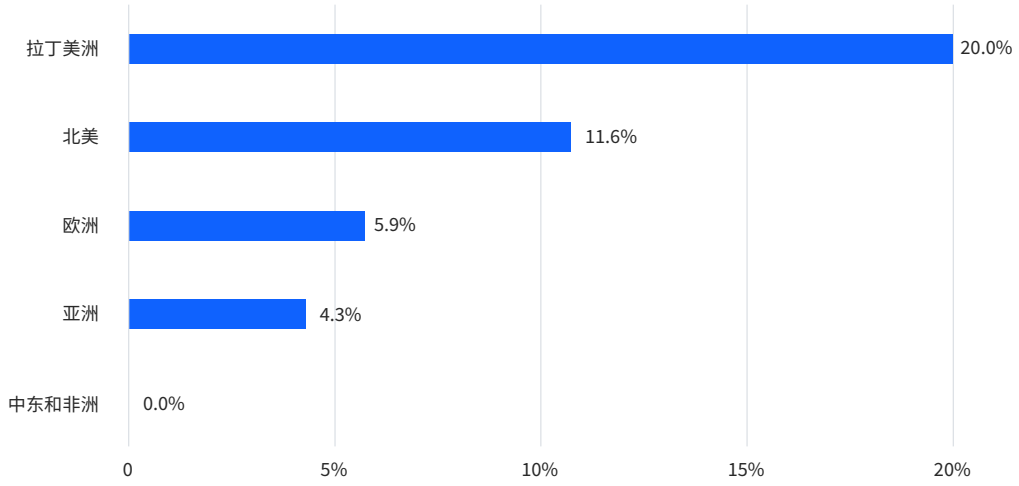
在 2020 年商务电子邮件泄露 (BEC) 攻击有所衰退之后，X-Force 观察到这类攻击数量在 2021 年再次减少。BEC 是我们的 X-Force IR 团队修复的第三大常见攻击类型。去年，我们推测，多因素身份验证 (MFA) 的广泛实施使得 BEC 威胁实施者成功执行的攻击数量日渐减少。这一理论在 2021 年是成立的，因为 BEC 攻击者可能已通过将重心转移到并未广泛实施 MFA 的地区取得了更大的成功。

例如，在 X-Force IR 团队所修复的 BEC 攻击中，拉丁美洲的组织受到的冲击似乎最大。虽然北美组织仍然是 BEC 操纵者着重瞄准的目标，但我们所注意到的对拉丁美洲组织迅速激增的攻击数量表明，在地理位置上，BEC 攻击者已转移了其运营重点：2019 年，对拉丁美洲组织发起的攻击为零，而在 2020 年和 2021 年，BEC 攻击占比分别达到 19% 和 20%。

图 6

2021 年 BEC 事件百分比

2021 年各地区的 BEC 事件百分比（资料来源：IBM Security X-Force）



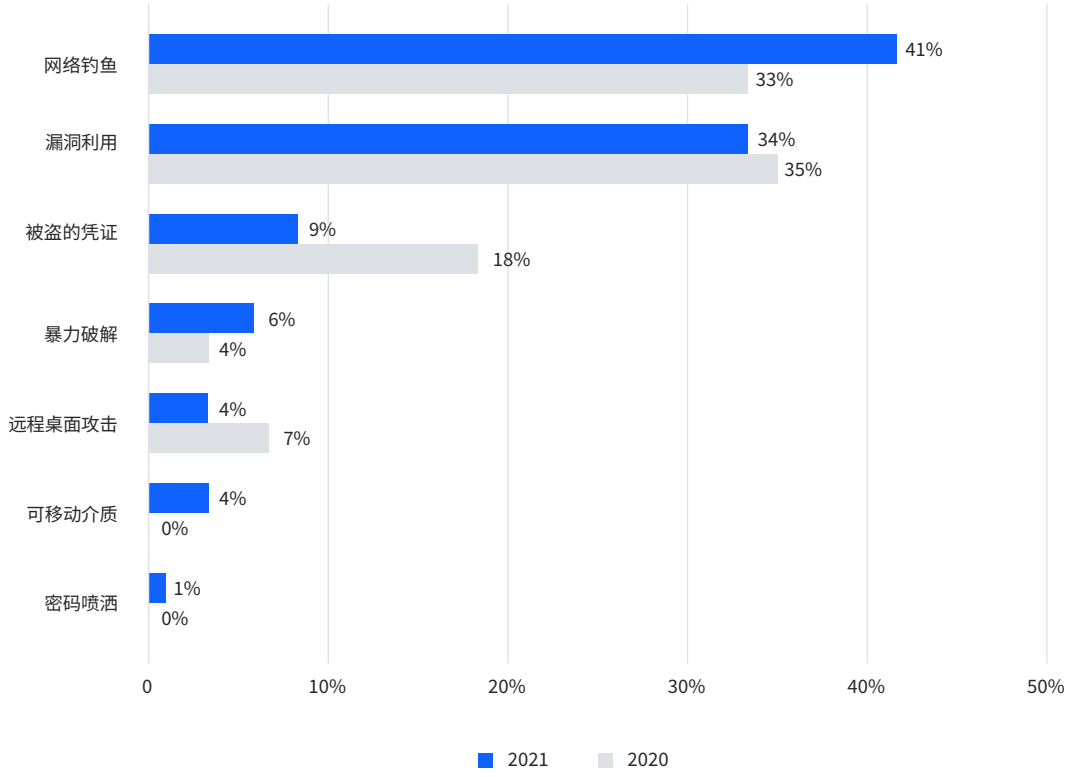
主要入侵媒介

除了检查 X-Force 观察到的威胁实施者的最终目标之外，我们的团队还跟踪威胁实施者通过何种方式获得受害者网络的初始访问权限。网络钓鱼和漏洞利用往往是我们观察到的最常见的方法，其次就是使用被盗凭证、暴力破解、远程桌面协议 (RDP)、可移动介质和密码喷洒，它们只占入侵行为的一小部分。

图 7

2021 年与 2020 年主要感染媒介对比

X-Force 事件响应团队观察到的感染媒介细分，2020-2021（资料来源：IBM Security X-Force）



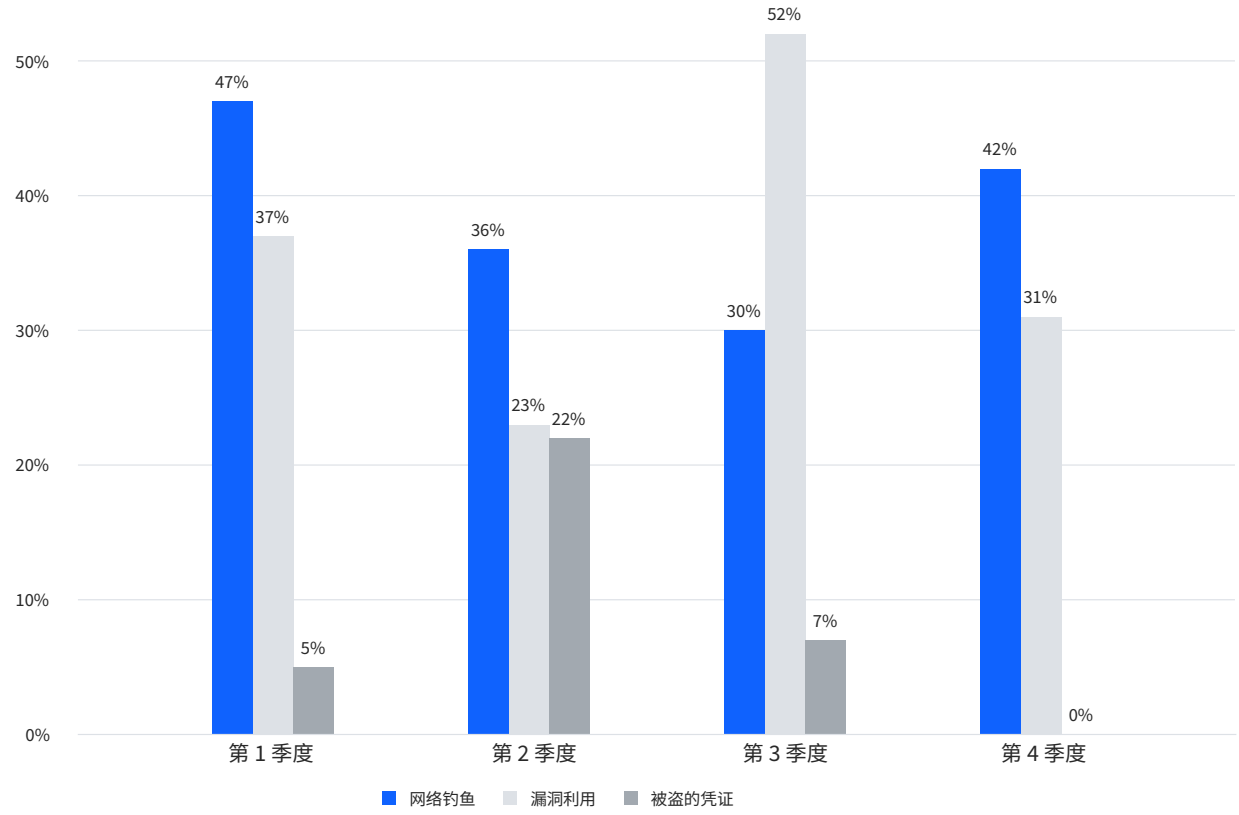
网络钓鱼

网络钓鱼成为 2021 年的首要感染媒介，超越了 2020 年领先的漏洞利用。据观察，在 X-Force 修复的事件中，网络钓鱼事件占到了 41%。尽管漏洞利用攻击在 2021 年第三季度占主导地位，但 X-Force 在第一季度和第四季度观察到的大量与网络钓鱼相关的事件将这种感染媒介推向了今年的头把交椅。

图 8

2021 年各季度与网络钓鱼、漏洞利用和被盗凭证相关攻击的百分比

2021 年各季度与各种感染媒介相关攻击的百分比（资料来源：IBM Security X-Force）



X-Force Red 的部分重点领域包括通过网络钓鱼电子邮件进行社会工程渗透测试攻击。对于 2020 年和 2021 年有针对性的网络钓鱼活动，X-Force Red 模拟活动的平均点击率为 17.8%。而将网络钓鱼（语音钓鱼）电话添加到活动中时，点击率上升到 53.2%，是原先的三倍。

BEC 攻击者已利用网络钓鱼活动和社会工程取得了巨大的成功。特别是在 2021 年，X-Force 发现勒索软件实施者更加依赖于网络钓鱼活动来获得受害者网络的初始访问权限，进而发起勒索软件攻击。

例如，2021 年观察到的多起 REvil 勒索软件事件都始于 QakBot 网络钓鱼电子邮件。这些电子邮件通常包含十分简短的消息，通常涉及未支付的发票，有时甚至会劫持正在进行的电子邮件对话，仅用恶意的附件来回复所有人。

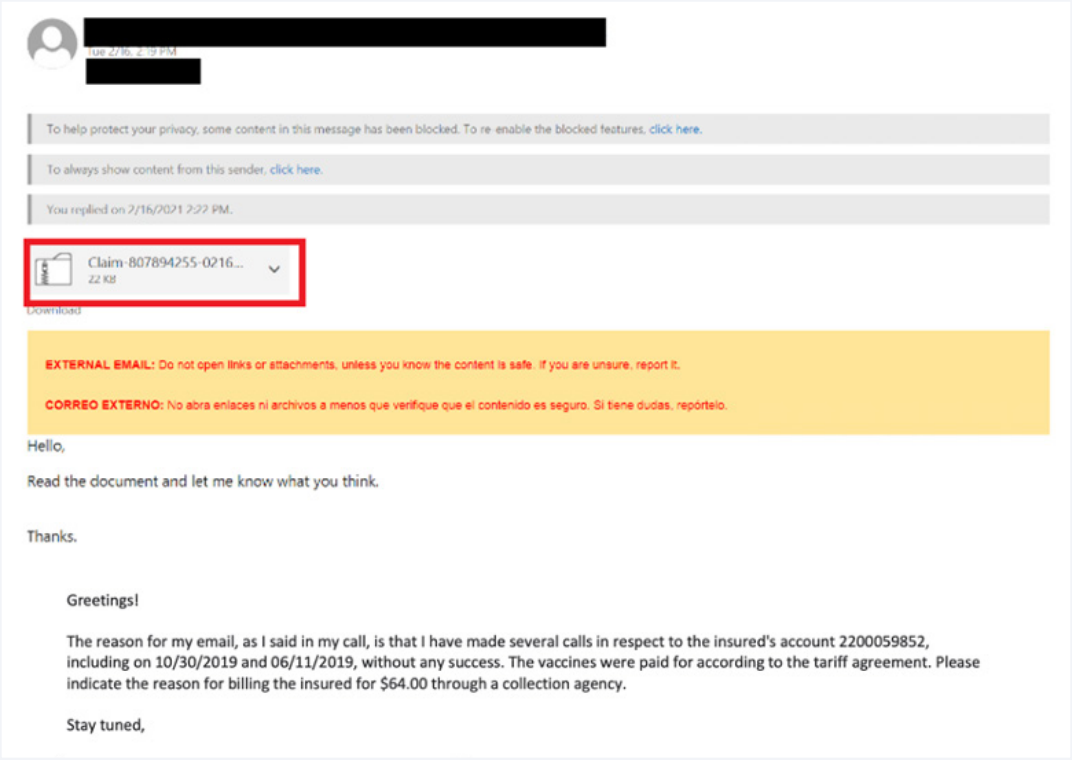
一经打开，该文档便将指示收件人启用宏，这将植入 QakBot 银行木马，从而在系统上初步获得立足之地。随后，操作权便会转交给 REvil 勒索软件实施者，他们会暗中进行侦察，并由此继续执行操作。

图 9 中包含了一个 QakBot 网络钓鱼电子邮件样本。

图 9

QakBot 网络钓鱼电子邮件样本

带有恶意附件的 QakBot 网络钓鱼电子邮件示例（资料来源：IBM Security X-Force）

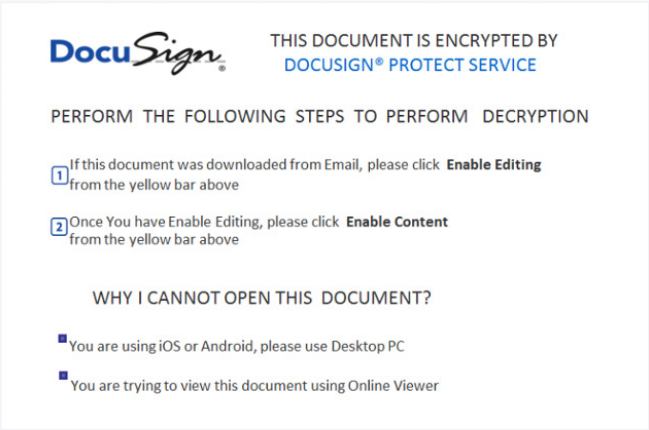


当收件人尝试打开附件时，会弹出一个提示框（参见图 10），要求通过选择“启用编辑”和“启用内容”来启用宏。这样一来，在恶意宏的帮助下，威胁实施者便能在受害者的机器上部署恶意软件。

图 10

来自 QakBot 网络钓鱼附件的弹出消息样本

恶意附件中提示收件人启用宏的消息（资料来源：IBM Security X-Force）



网络钓鱼工具包部署通常昙花一现、滥用技术且波及众多品牌

IBM 分析了来自世界各地的数千个网络钓鱼工具包，目的是确定这种特定攻击媒介的频率和有效性。我们的调查表明，使用网络钓鱼工具包的恶意行为者可能会耗费大量时间而只获得有限的收益。尤其是，我们的调查显示：

- 网络钓鱼工具包部署的寿命通常很短，几乎三分之一的部署工具包的使用时间不超过一天。在某些情况下，单个网络钓鱼工具包部署仅持续了 7 到 8 个小时，然后大多数托管服务提供商便会将该站点识别为恶意站点并加以阻止。
- 对于每次部署，平均只有不超过 75 名潜在受害者会访问该站点。
- 几乎在所有观察的网络钓鱼工具包（接近 100%）中，都会要求用户提供凭证（电子邮件/ID/密码组合），其次是信用卡数据（61%）请求）、邮寄地址 (40%)、电话号码 (22%)、出生日期 (17%)、身份证号码 (15%)、安全问题 (14%) 和 ATM PIN (3%)。

此外，X-Force 还研究了哪些品牌最常受到网络钓鱼工具包的欺骗。主要品牌包括大型科技公司和大型金融机构。排名前 11 位的品牌如下所示。

2021 年最常受到欺骗的前 11 个品牌

1. Microsoft
2. Apple
3. Google
4. BMO Harris Bank (BMO)
5. Chase
6. Amazon
7. Dropbox
8. DHL
9. CNN
10. Hotmail
11. Facebook

2021 年 6 月，
网络钓鱼攻击次数高达
222,127 次，
创下历史新高

反网络钓鱼工作组 (APWG) 指出，2021 年仅 6 月一个月的网络钓鱼攻击次数就达到 222,127 次，创下了历史新高。因而，X-Force 十分肯定地表示，由于易于使用的性质且只需少量资源，威胁实施者仍将会继续使用网络钓鱼工具包。监控可能的假冒品牌的可疑连接，可以帮助组织最大限度地降低遭受这种攻击媒介影响的概率。

使用专门用于保障数据隐私的 DNS 服务（如 Quad9[2]），也可以帮助降低网络钓鱼攻击的风险。

[2] IBM Security X-Force 是 Quad9 合作伙伴。

漏洞利用

尽管在 2021 年的最常见攻击排行榜上已下降到第二位，但在过去一年由漏洞利用引发的攻击事件数量与 2020 年相比仍增加了 33%，这表明这种攻击媒介在威胁实施者的武器库中还是有着举足轻重的地位。利用这一媒介，威胁实施者可以访问受害者网络，谋划进一步的操作——在许多情况下，他们所具有的权限都得到了提升。

X-Force 发现，攻击者往往会利用多个已知漏洞，例如 CVE-2021-35464（Java 反序列化漏洞）和 CVE-2019-19781（Citrix 路径遍历缺陷），以此获得对感兴趣网络的初始访问权限。此外，我们还观察到，威胁实施者在 Kaseya 勒索软件攻击和 Microsoft Exchange Server 事件等主要攻击中利用零日漏洞来访问受害者的网络和设备。

临近 2021 年年底时，对 Log4j 漏洞 CVE-2021-44228 的广泛利用，也促使该漏洞在 2021 年 X-Force 前十大漏洞名单中蹿升至第二位。您的组织可以利用一些缓解措施来避免成为该漏洞的受害者。

漏洞数量再创新高

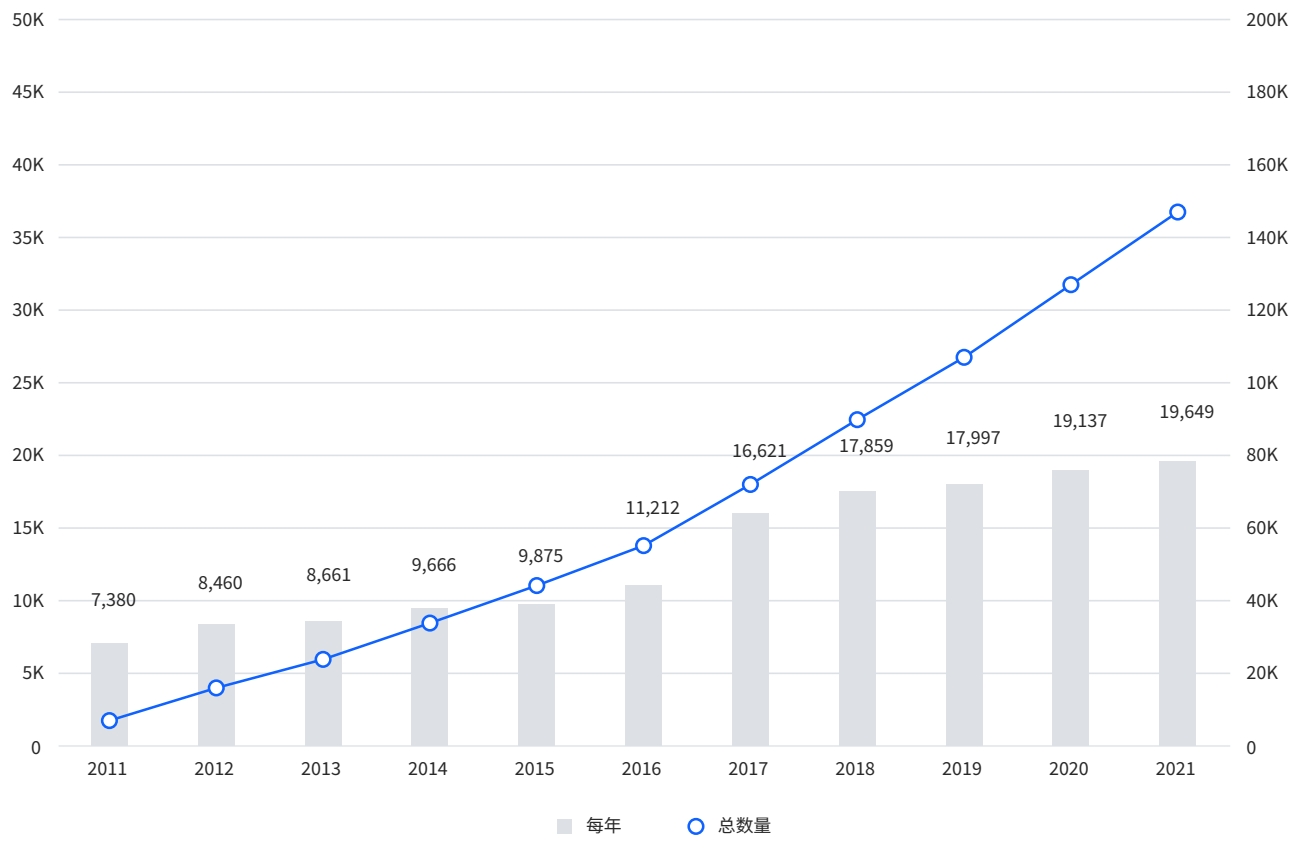
在过去五年里，漏洞数量以肉眼可见的速度逐年稳步增长。而更令人担忧的是，威胁实施者借以利用漏洞的工具数量也在稳步增长，阵列不断扩大，这让威胁实施者在寻求利用漏洞时便有了更多的选择。

与物联网 (IoT) 和工业控制系统 (ICS) 相关漏洞的增长速度甚至比整体漏洞增速还要快，这两类漏洞的年增长率分别为 16% 和 50%，而整体漏洞数量的增长率则为 0.4%。

图 11

2011-2021年每年发现的漏洞数量

2011-2021年每年新识别的漏洞数量和累计漏洞数量（资料来源：IBM Security X-Force）



2021 年的十大漏洞

任何漏洞都带有一定的风险，应加以评估。以下列表包含了 X-Force IR 团队观察到的威胁实施者在 2021 年运营过程中已利用或试图利用的主要漏洞。如果您的组织尚未修补这些漏洞，X-Force 建议您优先对这些漏洞加以修补。

1. CVE-2021-34523 – Microsoft Exchange 服务器缺陷，恶意行为者由此能够绕过身份验证并冒充管理员。一般称为 ProxyLogon。
2. CVE-2021-44228 – Apache Log4j 库中的漏洞
3. CVE-2021-26857 – Microsoft Exchange Server 远程代码执行漏洞
4. CVE-2020-1472 – Netlogon 提权漏洞
5. CVE-2021-27101 – 易受 SQL 注入影响的 Accellion FTA 漏洞
6. CVE-2020-7961 – Liferay Portal 对不可信数据的反序列化，允许通过 JSON 网络服务远程执行代码
7. CVE-2020-15505 – MobileIron 漏洞，允许远程执行代码
8. CVE-2018-20062 – NoneCMS ThinkPHP 远程代码执行漏洞
9. CVE-2021-35464 – ForgeRock AM 服务器 Java 反序列化漏洞，允许远程执行代码
10. CVE-2019-19781 – Citrix 服务器路径遍历缺陷

与工业控制系统 (ICS) 及更进一步的运营技术 (OT) 有关的已知漏洞以及物联网 (IoT) 漏洞正逐年增长，从 2020 年到 2021 年，已识别的漏洞数量增长幅度相当可观。

随着在数字化和互联网协议的强大力量作用之下，越来越多的“事物”开始联网，新的漏洞和风险也随之而来。虽然其中的许多问题仅影响工业组织，但只要在其基础架构中使用物联网，组织所面临的风险也就会有增而无减。

除了这种日益推进的数字化进程之外，动态变化的供应链也正在对许多涉及 OT 的组织的攻击面产生影响。威胁实施者深知制造和能源行业在全球供应链中发挥的关键作用，因而伺机破坏这些组织，这可能会对多个行业产生连锁反应，而这些倍增效应则会促使受害者迫于沉重的压力不得不支付赎金。

威胁实施者加快对 OT 设备的侦察速度

在分析了 2021 年的数据后，X-Force 发现攻击者正在开展大规模的侦察活动，在工业网络中四处寻找可利用的通信机会。具体来说，2021 年针对 TCP 502 端口的侦察活动已显著增加。

此端口使用 Modbus，这是一种应用层消息传递协议，用于在工业网络中连接的总线、网络和可编程逻辑控制器 (PLC) 设备之间提供客户端到服务器的通信。数据采集与监视控制系统通常会使用 502 端口。威胁实施者可以通过访问 Modbus 来控制连接到互联网的物理设备。

在 2021 年 1 月至 9 月期间，X-Force 观察到针对 502 端口的对抗性侦察活动增加了 2204%。

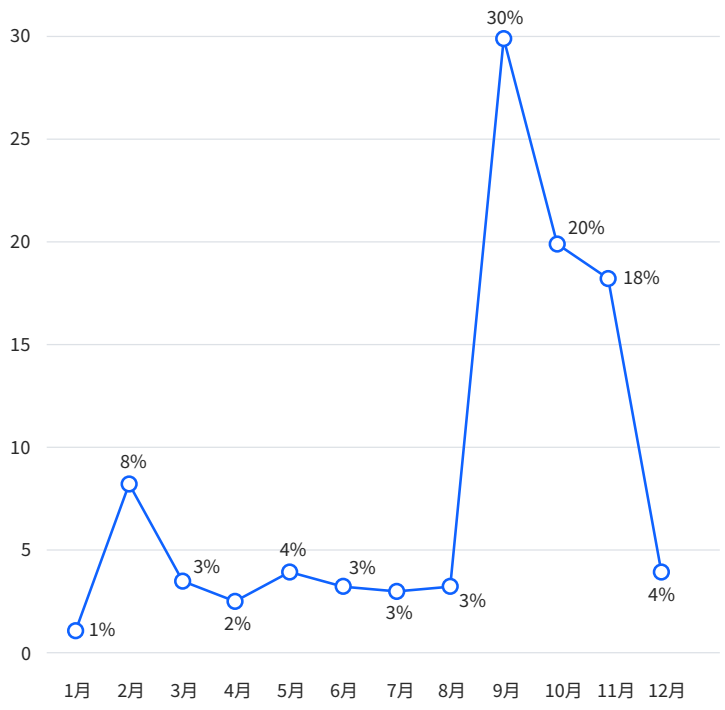
威胁实施者可能已经加强了 Modbus 侦察活动，开始寻找目标实施勒索，或者夺取控制权并造成伤害。鉴于 Modbus 缺乏安全功能，一旦攻击者找到可访问的 Modbus 设备，他们就可以向设备发出有害命令，并影响连接的 ICS 或 IoT 系统。

尽管 SCADA Modbus 位于 ICS 环境中 Purdue 模型的第 2 级（理想情况下应与企业网络相隔离，并放置在非军事区之后），但在某些情况下，可以通过开放的互联网直接访问 SCADA Modbus 502 端口。与其他更现代的技术相比，缺乏身份验证和纯文本消息传输则让 Modbus 的危险程度又增加一分。

图 12

2021 年按月细分的 SCADA Modbus 侦察量

2021 年 SCADA Modbus 侦察活动的逐月细分（资料来源：IBM Security X-Force）



制造业是 OT 行业中遭受攻击最多的行业，主要是勒索软件攻击

就拥有 OT 网络的行业而言，X-Force 观察到在 2021 年，制造业遭受的攻击次数最多，显著高于其他行业，并且在 X-Force 协助修复的事件中占到了 61%。制造业对于勒索软件实施者有着特殊的吸引力，这可能是因为这些组织对宕机时间的容忍度很低。

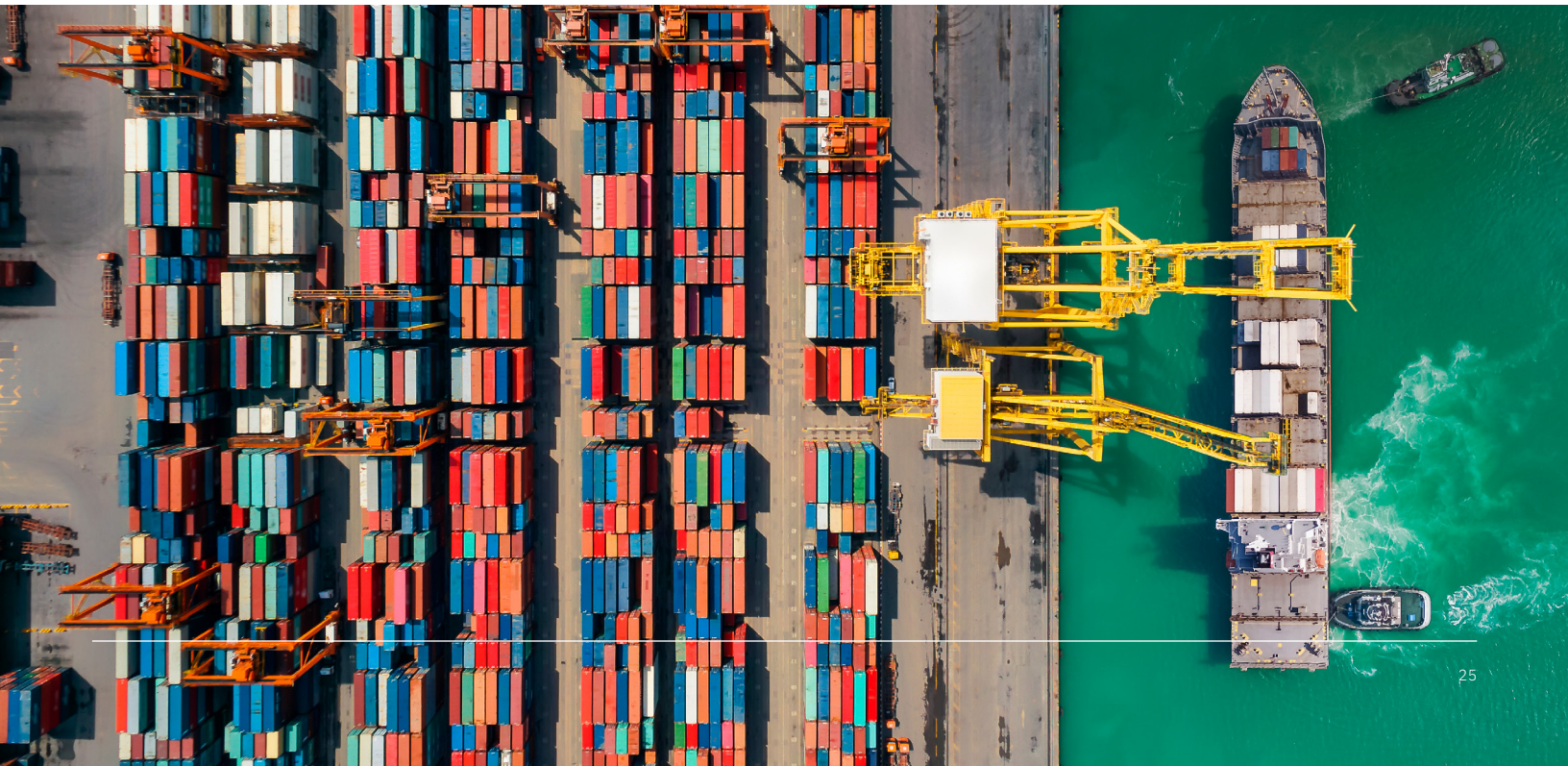


图 13

2021 年瞄准的 OT 行业

X-Force IR 在 2021 年观察到的六大运营技术行业遭受的攻击细分（资料来源：IBM Security X-Force）

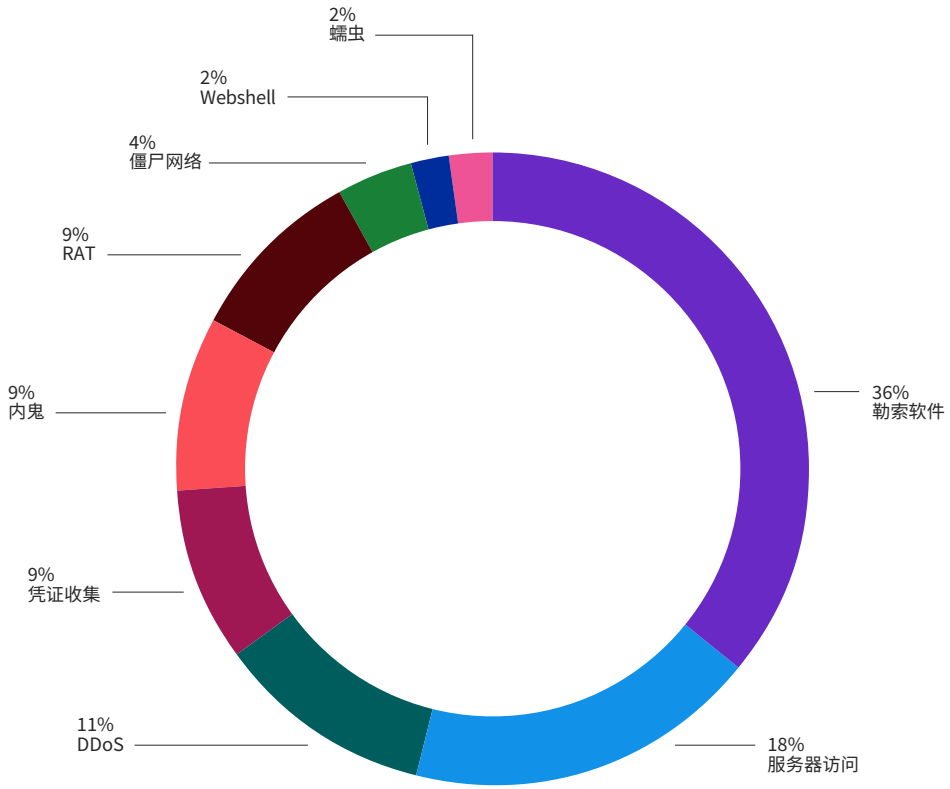
对于 X-Force 在 2021 年发现遭受攻击的所有具有 OT 网络的行业，包括工程、采矿、公用事业、石油和天然气、运输和制造行业，勒索软件在众多攻击类型中再次稳坐头把交椅，占全部攻击总量的 36%，这与所有行业的整体攻击趋势相呼应。虽然在绝大多数此类攻击中受到损害的都是 IT 网络，但在许多情况下，影响仍波及受害者的运营技术。

其他主要攻击类型包括服务器访问、DDoS、RAT、内部人员和凭证收集操作。

图 14

2021 年 OT 遭受的攻击类型

2021 年运营技术遭受的攻击类型细分（资料来源：IBM Security X-Force）



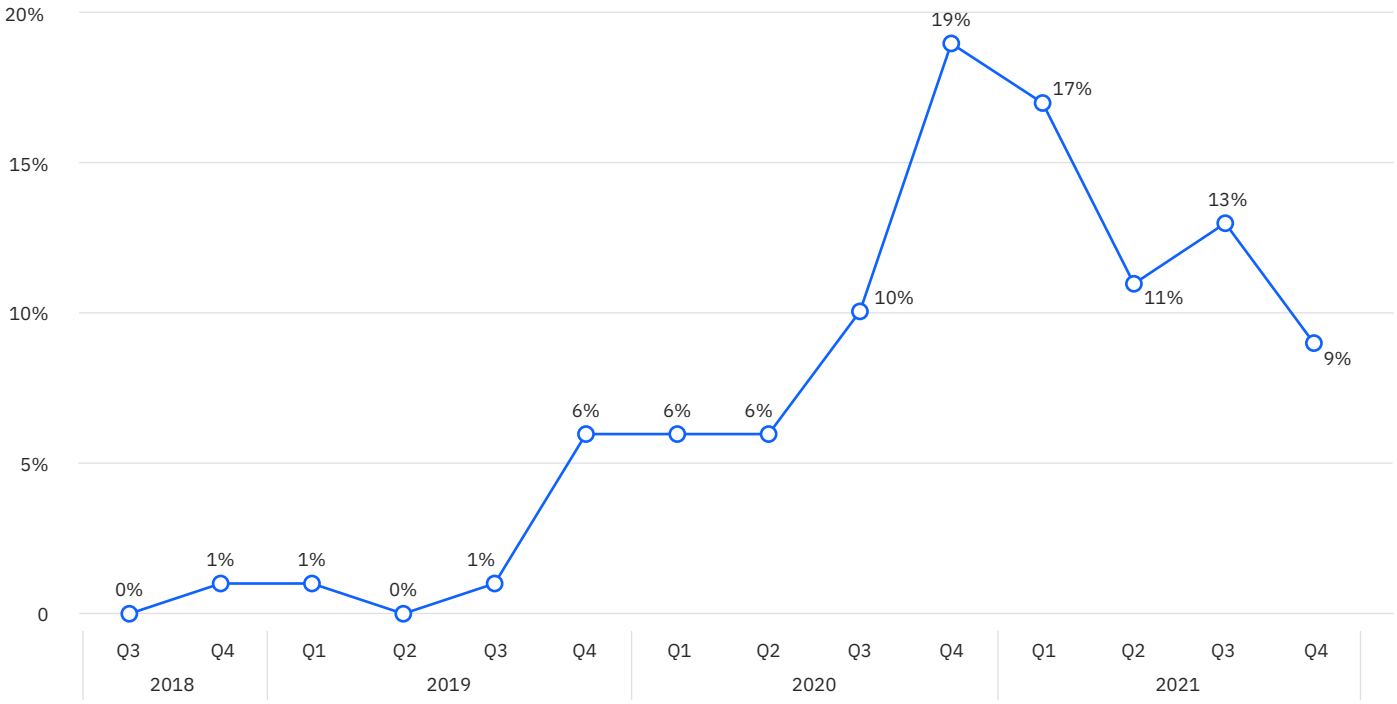
Mozi 僵尸网络仍对 IoT 和 OT 资产造成威胁

自 2019 年以来，X-Force 已发现大量 IoT 恶意软件活动，而在 2019 年第三季度至 2020 年第四季度期间，激增幅度已接近 3000%。与所有其他 IoT 恶意软件类型相比，Mozi 僵尸网络仍在 IoT 恶意软件阵营中占据大头，在 2021 年 X-Force 所观察到的 IoT 恶意软件总量中占到了 74%。

图15

2018-2021 年各个季度的 IoT 攻击量

2018-2021 年各个季度的 IoT 恶意软件活动占比（资料来源：IBM Security X-Force）



Mozi 滥用 Telnet 弱密码并利用漏洞来锁定网络设备、IoT 和录像机以及其他联网产品。感染之后，它能够持久留存在网络网关上，这可以作为特别有效的初始接入点，进而横向移动到一些高价值网络，包括 OT 和 ICS 网络。此外，通过感染路由器，Mozi 背后的威胁实施者可以发起中间人攻击，最终部署勒索软件，这包括对 OT 网络的攻击。

除了 Mozi 的访问和横向移动能力之外，一个感染了组织中大量安全摄像头或类似 IoT 设备的大型 Mozi 僵尸网络可能会降低组织有效执行物理安全操作的能力。

据报道，中国执法部门于 2021 年 6 月和 8 月逮捕了 Mozi 僵尸网络的始作俑者，而 2021 年第四季度 IoT 攻击量的下降可能就是这些逮捕行动产生的附带影响。

2021 年的主要威胁实施者

我们的 2021 年 IR 数据显示，在可识别威胁实施者的场景下，网络犯罪分子是发起攻击的主力军。

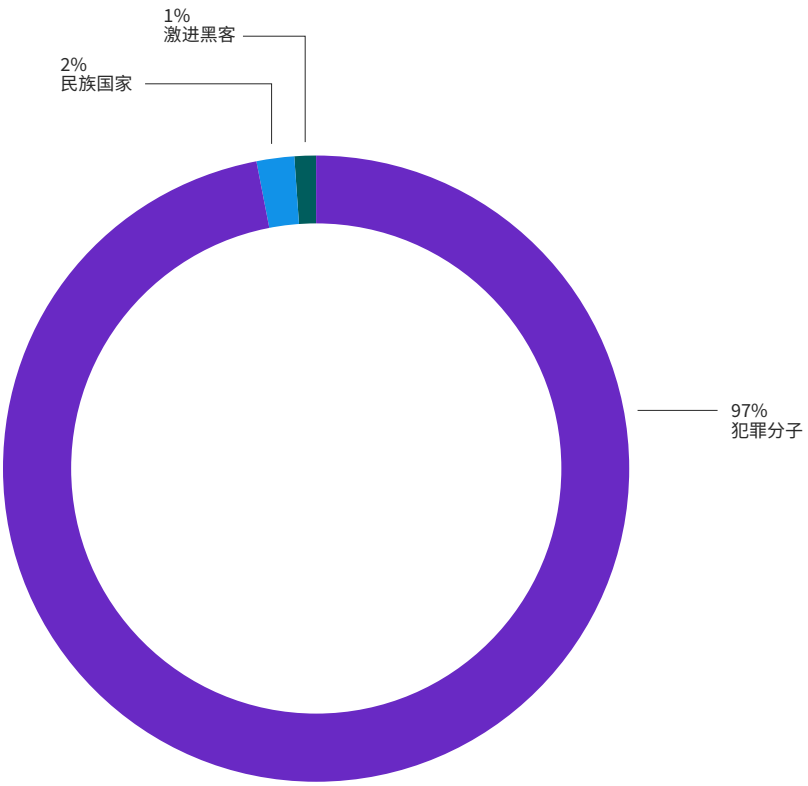
在 2021 年 X-Force 参与修复的事件中，民族国家行为者仅占 2%，其中的大量活动都是由网络犯罪活动所引发的。我们所观察到的民族国家行为者主要是在寻求开展间谍和监视活动，在某些情况下，可能一直在为未来的蓄意破坏活动打基础。我们发现，只有 1% 的攻击活动是由黑客组织发起的。

以下部分介绍了 X-Force 在 2021 年观察到的一些更有趣的活跃威胁组织的更多详细信息。

图 16

2021 年 X-Force 事件响应团队观察到的威胁实施者

2021 年 X-Force IR 观察到的威胁实施者团伙，按类型细分（资料来源：IBM Security X-Force）



疑似位于伊朗的 ITG17 使用 Aclip 后门

2021 年，IBM Security X-Force 团队发现一个威胁实施者使用了一个新后门，X-Force 将其命名为“Aclip”。此外，该攻击者还利用了合法的消息传递和协作应用工具，这可能会混淆运营通信，让恶意流量或具有潜在恶意意图的流量不被察觉。根据所观察到的工具、策略和基础架构，我们在一定程度上认为，所追踪的威胁实施者 ITG17[3]（又名 MuddyWater）疑似一个伊朗民族国家组织，它就是此次攻击活动的幕后黑手，其动机可能就是进行监视。

ITG23（Trickbot Gang）启用 Conti 勒索软件操作

X-Force 分析师一直在密切跟踪 Trickbot 银行木马背后的网络犯罪集团——我们将其称为 ITG23，也称为 Wizard Spider 或 Trickbot Gang。携带 Trickbot 特洛伊木马的网络钓鱼电子邮件通常被用作 Conti 勒索软件的切入点，据 X-Force 发现，ITG23 Trickbot 活动的增长正好与 Conti 勒索软件攻击的增长相吻合。

该团伙主要依赖电子邮件活动发送恶意 Excel 文档，以及臭名昭著的 BazarCall 活动，此时围绕订阅主题的电子邮件会怂恿收件人联系欺诈性的呼叫中心，然后话务员会以取消订阅服务为幌子，引导用户下载 BazarLoader 恶意软件。此外，该组织最近一直在劫持电子邮件线程，然后用恶意附件来回复所有人。

Hive0109 在 2021 年十分活跃

在 2021 年，X-Force 发现了多起 Hive0109（也称为 LemonDuck）攻击，事实已证明，该团伙十分擅长利用 ProxyLogon 漏洞来攻陷那些未打补丁的 Microsoft Exchange 服务器。LemonDuck 以 Linux 和 Windows 系统为目标，众所周知，它在攻击活动中主要是以具有新闻价值的事件作为网络钓鱼的诱饵。

LemonDuck 是一种持久存在的恶意软件，主要用于挖掘加密货币。它最晚可能自 2018 年起就在网络上活跃，并日渐演变成一个大型僵尸网络。LemonDuck 传播速度很快，并且可作为后续恶意软件和攻击的先头部队。它仍在受感染的设备上挖掘加密货币。

[3] ITG 表示 IBM Threat Group。这是 IBM X-Force 关于威胁实施者团伙（包括民族国家行为者和网络犯罪分子）的命名约定。IBM 以数字方式跟踪和命名威胁团伙，用 IBM Threat Group (ITG) 后跟分配的编号来识别。对于仍处于研究阶段的威胁团伙，我们使用 Hive 名称，如本节讨论的 Hive0109。

恶意软件发展趋势

威胁实施者不断创新并寻找新方法，让恶意软件在操作系统中展现更强的能力，且更加难以检测。本节介绍了 X-Force 在 2021 年观察到的一些恶意软件发展趋势。

更高的检测规避能力

X-Force 的恶意软件逆向工程团队在去年发现，恶意软件的规避技术已实现了重大升级。

- 勒索软件开发者使用不同的加密技术来规避基于主机的检测系统。间歇性加密就是一个例子，在这种情况下，会加密多个分开的数据块而不是整个系统，这就加快了加密过程。
- 指挥与控制 (C2) 通信日渐使用流行的云消息传递和存储服务来融入合法流量。此外，使用 DNS 进行隧道 C2 通信也变得越来越普遍。这些技术可帮助攻击者将 C2 活动伪装成合法通信，从而躲避基于网络的传感器的检测。
- 恶意软件开发者使用越来越复杂的打包和代码混淆技术来隐藏恶意软件的真正意图并阻止分析技术的运用。恶意软件开发人员还尝试了不同的编程语言，例如 PureBasic 和 Nim，目的就是加大逆向工程的难度。

恶意软件着重关注 Docker

通过分析影响云环境的恶意软件发展趋势，X-Force IR 团队发现，多个恶意软件家族都将目光从通用 Linux 系统转移到 Docker 容器上，这些容器通常用于平台即服务云解决方案。

显示这一转变的部分恶意软件家族包括 XorDDoS、Groundhog 和 Tsunami。这种以 Docker 为重点的攻击不仅涉及机器人，还强调了 IoT 恶意软件 (Kaiji)、加密矿工 (Xanthe、Kinsing) 和其他恶意软件的恶意活动，它们都旨在利用云计算的力量来扩大其挖矿能力。

除 Docker 外，我们还发现威胁实施者也瞄准了其他容器平台。例如，我们发现 Siloscape 恶意软件破坏了易受攻击的 Windows 容器和 Kubernetes 容器管理平台。Siloscape 日渐被 TeamTNT 等威胁实施者纳入攻击武器库中，TeamTNT 是一个网络犯罪团伙，一直专注于云平台，企图扩大其加密劫持僵尸网络的影响范围。

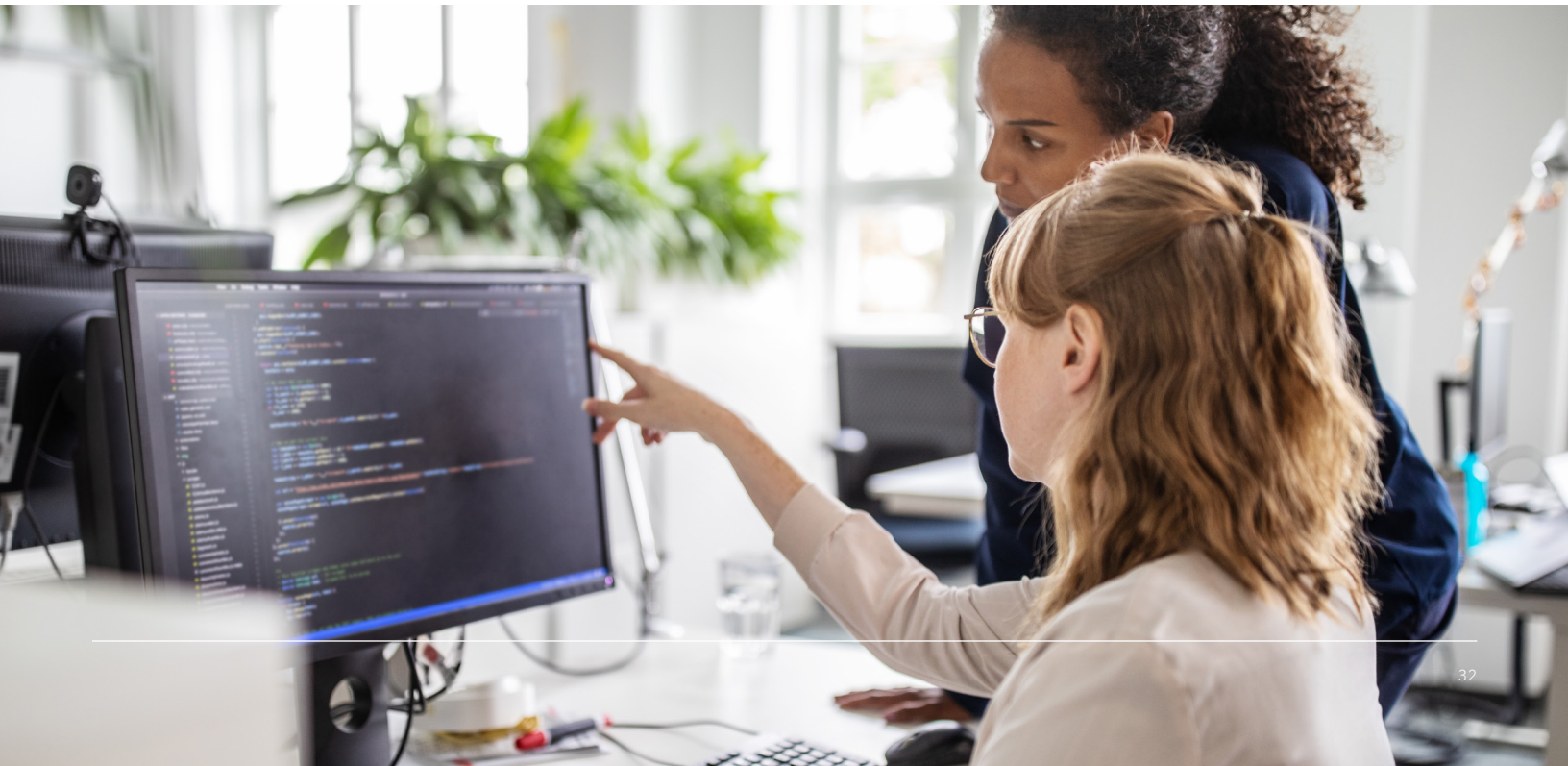
勒索软件着重关注 ESXi

通过分析影响 Linux 环境的恶意软件发展趋势，X-Force 发现，多个勒索软件家族都将目光转向基于 Linux 的 VMWare ESXi 服务器。随着越来越多的组织日渐依赖虚拟化技术，勒索软件开发者发现，与感染运行的操作系统相比，加密虚拟机 (VM) 文件本身显然更有效。

2020 年，X-Force IR 团队发现了针对 ESXi 服务器部署的 SFile 勒索软件的 Linux 变体。到了 2021 年，许多其他勒索软件家族似乎也纷纷效仿，这包括 REvil、HelloKitty、Babuk 和 BlackMatter。这些变体通常会使用 ESXi 自有的命令行管理工具 esxcli 来枚举和关闭运行的虚拟机，然后再进行加密。

Nim 日渐流行

2020 年，跨平台恶意软件开发人员倾向于选择 Golang 作为编程语言，因为它可以同时面向多个操作系统进行编译。虽然他们在 2021 年仍在使用 Golang，但 Nim 等其他语言正日渐流行起来。例如，威胁实施者使用 Nim 编译了 Nimar 后门以及 Zebrocy 版本，后者是俄罗斯民族国家行为者 ITG05（又名 APT28）使用的一种恶意软件类型。



Linux 威胁仍不断演变

据 IBM Security X-Force Threat Intelligence 合作伙伴 Intezer 的分析显示，在过去一年，针对 Linux 环境的恶意软件急剧增加，这表明威胁实施者对该领域仍然虎视眈眈。

Intezer 通过分析恶意软件种族的代码唯一性来衡量创新水平。具有更多独特变体的恶意软件代码表明，实施者已运用更高创新能力来编辑恶意软件，而重新使用大部分代码的恶意软件所具有的创新水平则较低。通过使用这种方法，最终得到了以下结果。

自去年以来，在多种类别的 Linux 恶意软件中，高达五分之四的恶意软件类别都增加了特有的代码，其中银行木马的增幅最大，其创新水平提升了十倍以上。Linux 目标的增多可能与组织正日益迁移到云环境有关，这些环境经常依赖 Linux 执行操作。

Linux 恶意软件的创新水平与基于 Windows 的恶意软件的创新水平不相上下，这凸显了 Linux 恶意软件运用创新的普遍程度，在 2022 年，我们肯定还会看到这一趋势仍保持上涨势头。

图 17

2021 与 2020 年具有独特代码的 Linux 恶意软件

2020-2021 年五大类别中具有独特代码的 Linux 恶意软件（资料来源：Intezer）

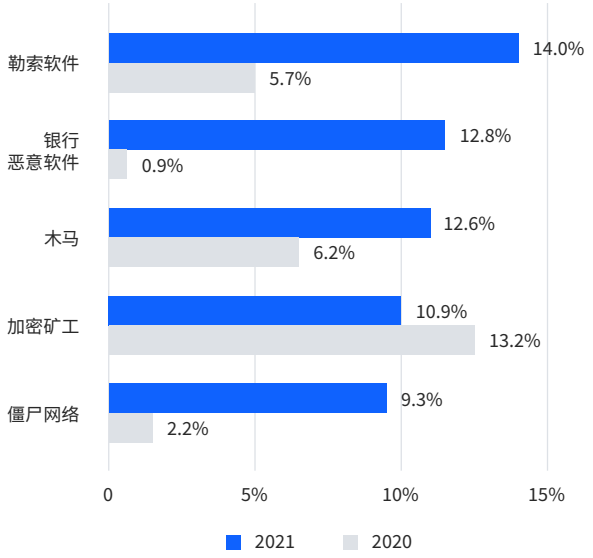
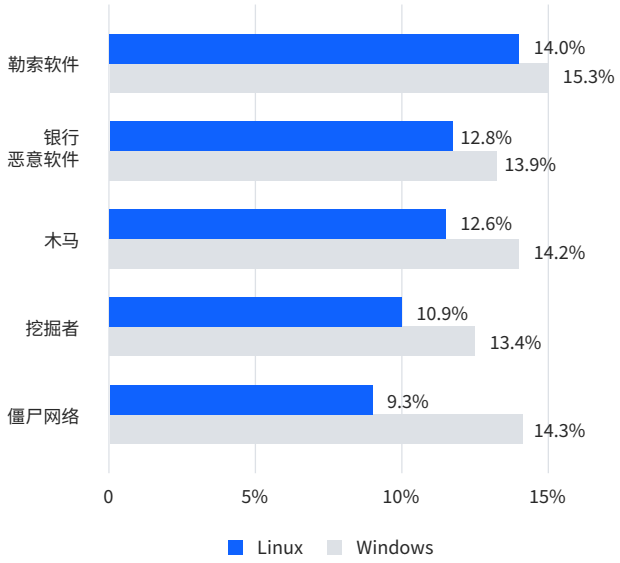


图 18

2021 年 Linux 与 Windows 中具有独特代码的恶意软件

2021 年新 Linux 恶意软件与新 Windows 恶意软件的比较（资料来源：Intezer）



威胁实施者以云环境为目标

IBM 对云安全威胁形势的研究着重表明，威胁实施者仍在不断努力将目标转移到云环境中。收集到的数据显示，威胁实施者使用了多种方法来获得组织云资产的初始访问权限，其中近四分之一的事件源于威胁实施者将目光从本地网络转向云环境。此外，研究的事件当中还有近三分之二的事件涉及 API 配置错误问题。这一目标的选择正好与庞大的云相关凭证地下市场相互印证，在这一市场上，数以万计的帐户都被挂在网上出售。

随着组织逐步迁移到云端，威胁实施者也紧随其后。维护适当强化的系统，制定有效的密码策略，并确保策略合规性，对于维持稳健的云安全态势有着举足轻重的作用。

云中的无文件恶意软件

通过利用合法的脚本语言和避免使用签名，潜伏在内存中的无文件逃避型恶意软件可以躲避标准检测工具的检查。X-Force 的研究发现，除了使用脚本来启动无文件恶意软件外，威胁实施者现在还使用 Ezuri，这是一种以 Golang 编写的开源加密程序和内存加载程序，它使得启动未经检测的恶意软件更加轻而易举。

X-Force 的研究还强调了一种名为 VermillionStrike 的新恶意软件套件的发展状况。VermillionStrike 基于流行的渗透测试工具 CobaltStrike；然而，与其对应工具不同的是，VermillionStrike 目的是在 Linux 系统上运行。这一发展变化强调了恶意软件正日渐将目光转投 Linux，可能也表明未来的操作仍将在 Windows 环境之外进行。

地理区域趋势

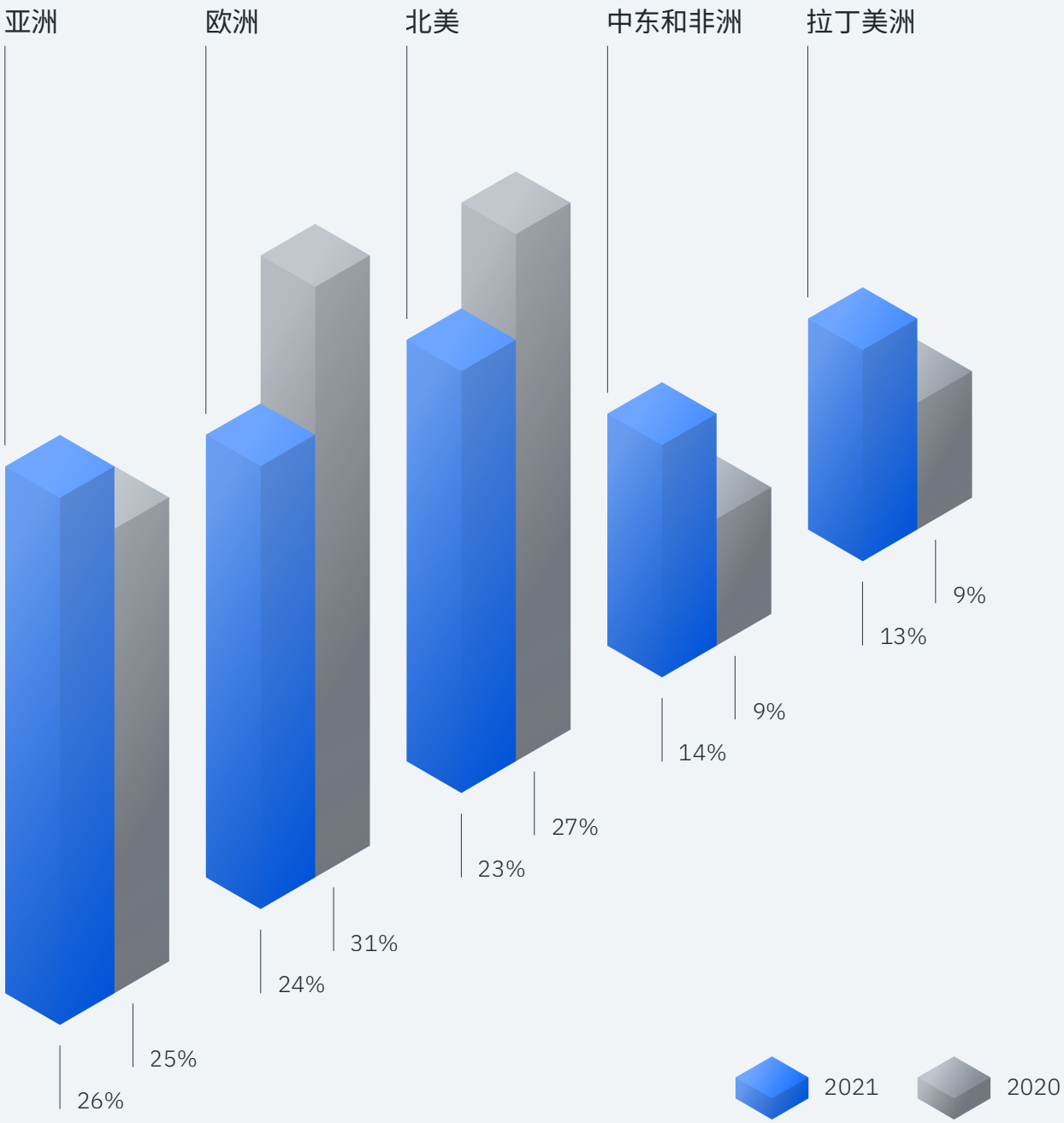
自本报告开始记录地理趋势以来，2021 年，亚洲首次成为攻击的重灾区，在 X-Force 去年所观察到的攻击总量中占到了 26%。尤其是针对日本的一连串攻击（可能与 2021 年在日本举行的夏季奥运会有关），似乎促成了这一攻击趋势。

欧洲和北美紧随其后，分别占攻击总量的 24% 和 23%，而中东和非洲与拉丁美洲所占比重则分别为 14% 和 13%。

图 19

2021 与 2020 年按地理位置细分的攻击情况

资料来源：IBM Security X-Force



亚洲

出于报告的目的，IBM 认为亚洲包括澳大利亚、东亚和东南亚、印度和太平洋岛屿。

服务器访问攻击 (20%) 和勒索软件 (11%) 是亚洲组织在 2021 年主要遭受的两种攻击类型，紧随其后的便是数据盗窃 (10%)。亚洲地区的服务器访问攻击占比很高，表明亚洲组织善于快速识别攻击，从而防止它们升级为更令人担忧的攻击类型。远程访问木马和广告软件并列第四，占攻击总量的 9%。

在亚洲，REvil 在 X-Force 所观察到的勒索软件攻击中占到了 33%，而 Bitlocker、Nefilim、MedusaLocker 和 Ragnar Locker 也是重要的参与者。

漏洞利用和网络钓鱼并列成为亚洲组织在 2021 年的主要感染媒介，据观察显示，该地区 43% 的攻击都由这两者引发而来。暴力破解 (7%) 和使用被盗凭证 (7%) 偶尔也会被用来获得网络的初始访问权限。

在亚洲，金融和保险组织最常受到攻击，在 X-Force 修复的事件中占到了 30%，紧随其后的是制造业 (29%)，然后就是专业和商业服务 (13%) 以及运输行业 (10%)。在全球范围内，据 X-Force 观察显示，金融和保险业是 2015 到 2020 年间遭受攻击次数最多的行业，因此，亚洲地区呈现出来的攻击趋势也是 X-Force 多年来观察到的这一全球趋势的延续。

日本、澳大利亚和印度是亚洲地区遭受攻击最多的国家。

遭受攻击最多的行业

1.	金融与保险	30%
2.	制造业	29%
3.	专业与商业服务	13%

欧洲

出于报告的目的，IBM 认为欧洲组织是位于西欧、东欧和土耳其的组织。

欧洲在全球最易遭受攻击地区排行榜上位列第二，遭受的攻击在 X-Force 事件响应团队所观察到的攻击中占到了 24%。勒索软件是欧洲面临的最主要的攻击类型，在 2021 年该地区遭受的攻击总量中占到了 26%。服务器访问 (12%) 位居第二，接下来便是数据盗窃 (10%)、配置错误 (8%)、恶意内部人员 (6%) 和欺诈行为 (6%)。勒索软件攻击者可能会被欧洲众多的高收入组织所吸引，这些组织由此就可能成为勒索软件的潜在攻击目标。2021 年，在欧洲遭受的勒索软件攻击中，REvil 攻击占比高达 38%，Ryuk 则占 25%。此外，我们还发现了 DarkSide、LockBit 2.0 和 Crystal 勒索软件团伙。这些勒索软件团伙倾向于捕捉“大型猎物”，或者瞄准属于大型财团的企业网络的重要部分，其终极目标就是攫取大笔赎金。

漏洞利用是针对欧洲组织主要使用的感染媒介，占据了 X-Force 在欧洲修复的事件总量的 46%，紧随其后的是网络钓鱼，占到了 42%。暴力破解则占事件总量的 12%。

制造业是 2021 年欧洲地区最常受到攻击的行业，占攻击总量的 25%，其次是金融和保险业 (18%)，再接下来便是专业和商业服务行业 (15%)。勒索软件攻击者对制造和专业服务组织的关注，可能正在推动这些趋势的进一步发展。

英国、意大利和德国是欧洲地区遭受攻击最多的国家。

遭受攻击最多的行业

1.	制造业	25%
2.	金融与保险	18%
3.	专业与商业服务	15%

北美

出于报告的目的，IBM 认为北美包括美国和加拿大。

2021 年，北美在全球最易遭受攻击地区排行榜上位列第三，遭受的攻击在 X-Force 事件响应团队所观察到的攻击中占到了 23%。与欧洲类似的是，勒索软件也是北美地区组织面临的头号攻击类型，占该地区攻击总量的 30%。由于该地区在 2021 年加大了执法力度，包括打击僵尸网络和勒索软件团伙，这可能影响了我们传统上所观察到的攻击率。

在 X-Force 于北美地区观察到的勒索软件攻击中，REvil 攻击占到了 43%，此外，X-Force 还发现了 LockBit 2.0、Conti、CryptoLocker 和 Eking。在北美地区，BEC 是仅次于勒索软件攻击的最常见攻击类型，占攻击总量的 12%，这表明 BEC 攻击者已重新开始对北美地区的组织发起攻击，试图入侵那些尚未部署 MFA 的组织。服务器访问攻击 (9%) 在北美地区组织最易遭受的攻击排行榜上位列第三。

网络钓鱼似乎是瞄准北美地区的威胁实施者首选的攻击媒介，在 2021 年 X-Force 在该地区修复的事件中占到了 47%。漏洞利用以 29% 的占比位列第二，此外，还使用了可移动介质 (12%)、暴力破解 (9%) 和被盗凭证 (9%) 这些攻击媒介。随着越来越多的北美地区组织针对 2020 年和 2021 年发布的若干关键漏洞实施稳健的补丁管理计划，威胁实施者可能会专注于网络钓鱼活动。

制造业是北美地区遭受攻击最多的行业，占 X-Force 修复的攻击总量的 28%——这一攻击率可能与疫情导致的制造业在供应链方面承受巨大压力有关。专业和商业服务行业以 15% 的占比位居第二，其次是零售和批发行业，占比为 11%。制造业、专业服务和批发行业都是勒索软件实施者争相追逐的目标，这可能是因为它们对停机时间的容忍度很低，而且其网络上保存有敏感的客户数据，如果不慎被盗并遭遇泄露危机，可能会给受害者带来巨大压力，最终不得不支付赎金。

遭受攻击最多的行业

1.	制造业	28%
2.	专业与商业服务	15%
3.	零售批发	11%

中东和非洲

出于报告的目的，IBM 认为中东和非洲包括黎凡特、阿拉伯半岛、埃及、伊朗和伊拉克，以及整个非洲大陆。

勒索软件和服务器访问攻击是中东和非洲最常遭遇的事件类型，它们并列第一，各占攻击总量的 18%。配置错误紧随其后，占 14%，凭证收集和 DDoS 攻击在该地区也相当普遍。

在 X-Force 于中东和非洲地区修复的已知初始感染媒介的事件中，50% 的事件都是由漏洞利用所引发的。使用被盗凭证和网络钓鱼也经常被用来访问感兴趣的中东和非洲地区网络，密码喷洒和使用可移动介质偶尔也会被用来获得初始访问权限。

在 2021 年针对中东和非洲地区发起的攻击中，金融和保险组织差不多扛下了半壁江山，遭遇的攻击占攻击总量的 48%，这表明该地区遭受的攻击可能已从由民族国家支持的以能源为重点的攻击转变为以金融组织为重点的网络犯罪攻击。沙特阿拉伯从利用原油收入发展经济转向实现经济多元化，可能也影响了这一趋势。医疗保健组织遭受的攻击占该地区所遭遇攻击总量的 15%，而能源组织则与该地区 10% 的攻击有关。

沙特阿拉伯、阿拉伯联合酋长国和南非是中东和非洲地区遭受攻击最多的国家。

遭受攻击最多的行业

1.	金融与保险	48%
2.	医疗卫生	15%
3.	能源部	10%

拉丁美洲

出于报告的目的，IBM 认为拉丁美洲包括墨西哥、中美洲和南美洲。

2021 年，拉丁美洲主要遭受的攻击类型就是勒索软件攻击，占攻击总量的 29%，其次便是 BEC（21%）和凭证收集（21%），这两类攻击在排行榜上并列第二。REvil 是我们在拉丁美洲观察到的最常见的勒索软件团伙，其发起的攻击次数占 X-Force 修复的勒索软件攻击量的 50%，此外，我们还发现，Ryuk 和 AtomSilo 也将黑手伸向该地区的组织。正如本文先前所述，针对拉丁美洲的 BEC 攻击率高于其他任何地区，并且自 2019 年以来急剧增加，这表明 BEC 攻击者正在集中更多精力在拉丁美洲寻找“猎物”。

网络钓鱼是威胁实施者在拉丁美洲搜寻“猎物”最常使用的感染媒介，这类攻击占 X-Force 在该地区所修复攻击量的 47%。通过网络钓鱼实施的大量 BEC 攻击和勒索软件攻击可能正在推动这一趋势的发展。被盗凭证导致的攻击占拉丁美洲的组织所遭受攻击量的 29%，这一比例明显高于其他地区，这表明更广泛地使用 MFA 有助于减少该地区的凭证被盗事件和 BEC 事件。在拉丁美洲的组织中，只有 18% 的攻击事件是由漏洞利用所引发的，而剩下的 6% 则是由可移动介质所导致的。

制造业是 2021 年拉丁美洲遭受攻击最多的行业，但只以 22% 的比例小幅领先。紧随其后的便是零售和批发业 (20%)、金融和保险业 (15%)，可能最令人惊讶的是，采矿业的占比也达到了 11%。拉丁美洲的专业和商业服务以及能源行业也遭到了相当严重的攻击。勒索软件攻击者和 BEC 攻击者似乎对这些行业很感兴趣，这可能会提高拉丁美洲地区这些行业遭受的攻击率。

巴西、墨西哥和秘鲁是拉丁美洲地区遭受攻击最多的国家。

遭受攻击最多的行业

1.	金融与保险	48%
2.	医疗卫生	15%
3.	能源部	10%

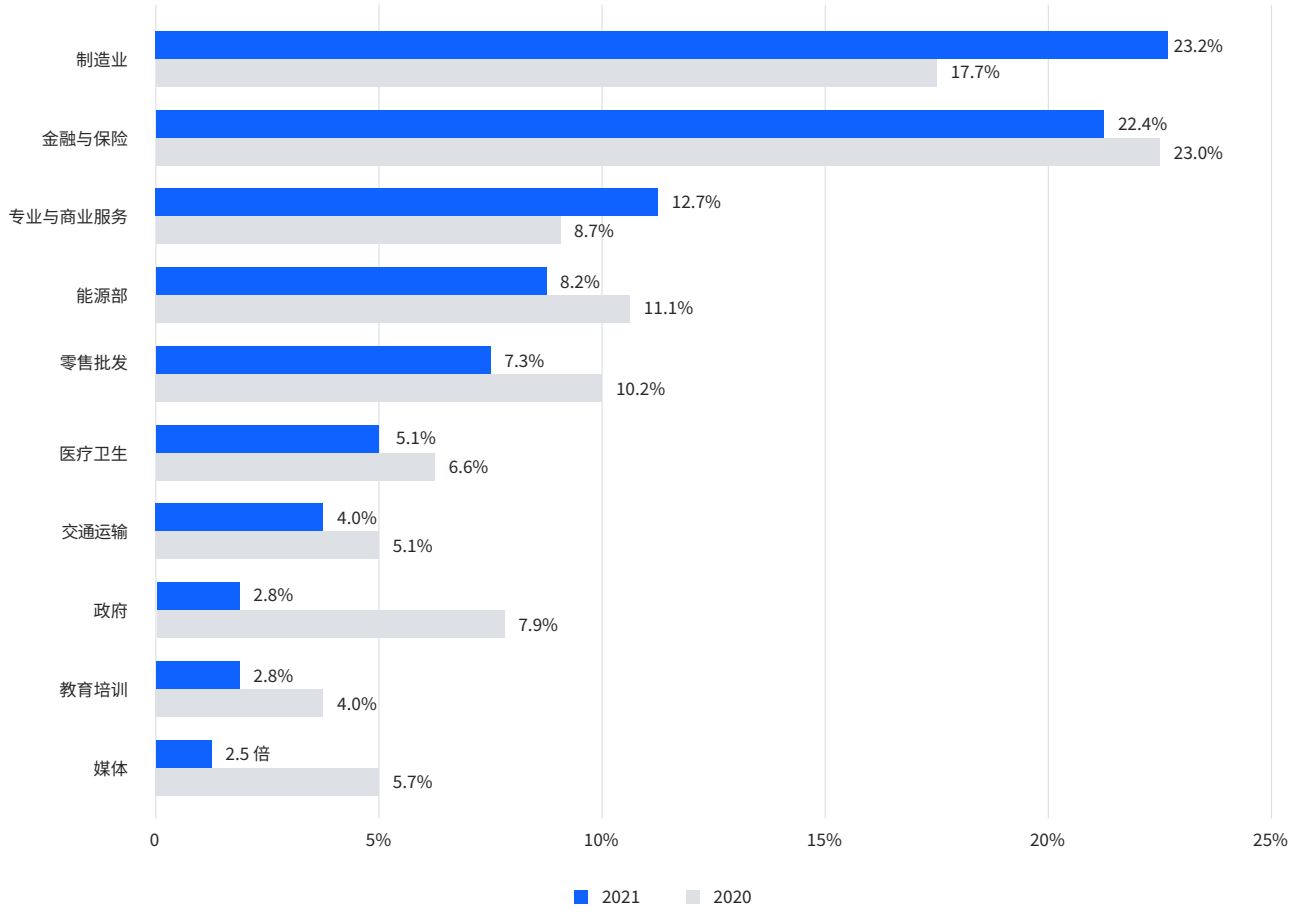
在本报告所研究的五年多的时间跨度里，2021 年，制造业首次成为遭受攻击最多的行业，金融和保险业则以小幅差距位列第二。针对制造组织发起的猛烈的勒索软件和 BEC 攻击，外加 COVID-19 疫情造成的供应链压力，可能促成了这一转变。

除金融和制造业外，专业和商业服务在 2021 年也成为了主要目标，尤其吸引了勒索软件实施者的注意。今年，我们正在将专业和商业服务以及零售和批发行业相结合，力求提供更广泛的行业攻击图景。值得注意的是，去年，批发行业遭受攻击的严重程度远远超过零售行业，这一行业的排名在很大程度上是由批发行业所推动的。我们希望确保在今年的排名中涵盖针对批发行业发起的攻击级别。

图 20

2021 年与 2020 年前 10 大行业遭受的攻击率

（资料来源：IBM Security X-Force）



#1 | 制造业

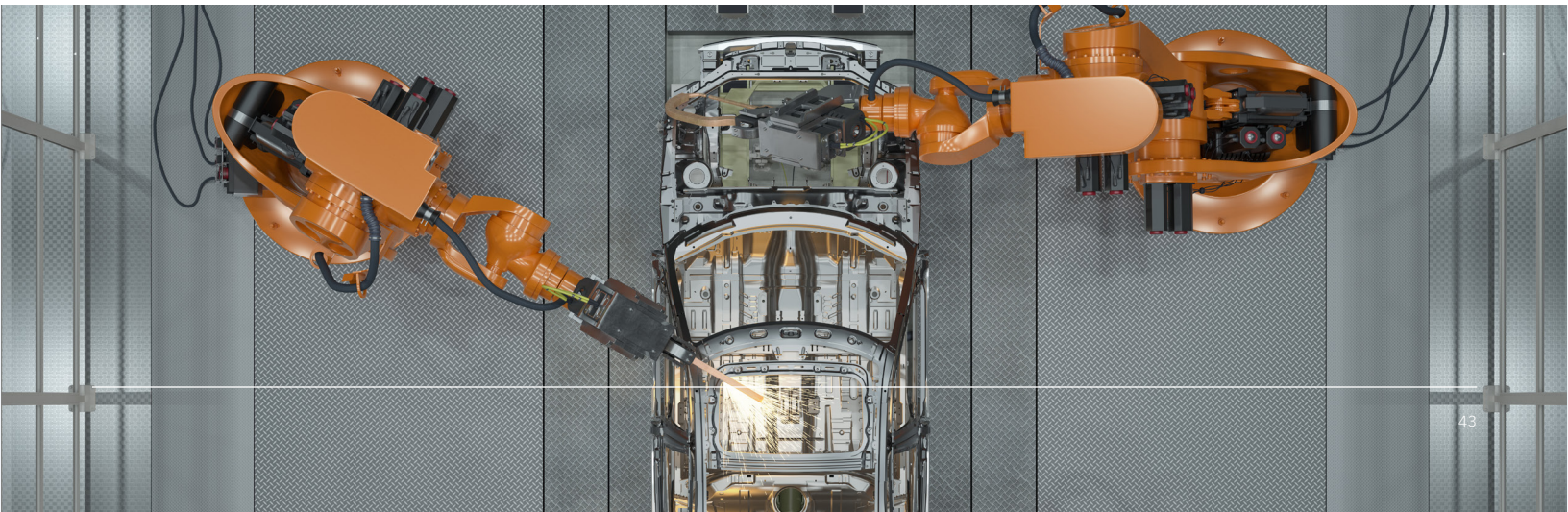
自 2016 年以来，制造业首次在 X-Force 的排名中位居第一，成为 2021 年遭受攻击最多的行业，在 X-Force 修复的攻击中占到了 23.2%。

勒索软件是最主要的攻击类型，占制造业组织所遭受攻击的 23%，这凸显了勒索软件实施者正将制造业视为主要攻击目标。服务器访问攻击以 12% 的占比位列第二，这可能代表了攻击者的一些失败操作。BEC 和数据盗窃并列第三，各占 10%。BEC 攻击者可能正在寻求利用制造业组织发展的众多供应商、次级供应商和批发运输关系，并试图将合作伙伴之间的付款重定向到由 BEC 攻击者控制的账户。数据盗窃可能旨在窃取敏感的知识产权，或者持有数据以勒索赎金。

漏洞利用是 2021 年制造业组织遭受攻击的最主要感染媒介，占比为 47%，紧随其后的是网络钓鱼，占比为 40%。这些数量庞大的攻击可能推动了 X-Force 在 2021 年观察到的整体初始感染媒介的发展趋势。可移动介质 (7%)、被盗凭证 (3%) 和暴力破解 (3%) 也占攻击的一小部分。尽管漏洞利用位居榜首，但除了漏洞管理之外，制造业组织可能还希望付出同等的努力来对抗网络钓鱼威胁。

2021 年，对制造业组织发起的攻击中，近三分之一 (32%) 的攻击活动发生在亚洲，北美 (27%) 和欧洲 (26%) 的攻击占比十分接近。拉丁美洲 (13%) 以及中东和非洲 (5%) 的制造业也遭到了攻击。

占攻击总量的 23.2%



#2 | 金融与保险

金融和保险组织也是攻击者追逐的目标，它们所遭受的攻击在 2021 年 X-Force 修复的攻击中占到了 22.4%，在 X-Force 的行业排名中稳居第二位。在这些攻击中，70% 的攻击针对银行，16% 针对保险机构，14% 则是针对其他金融机构。

占攻击总量的 22.4%

金融业从榜首跌落，这表明大多数金融机构所实施的高安全标准正在逐渐取得实效，金融服务业正在践行正确的安全之路。此外，混合云环境也在金融服务组织中占主导地位，这提高了敏感数据的可见性和管理水平。

2021 年，服务器访问攻击勉强成为金融和保险组织遭受的最主要攻击类型，占攻击总量的 14%。紧随其后的是勒索软件、配置错误和欺诈行为，它们以 10% 的占比并列第二。RAT、广告软件和凭证收集也是金融服务行业相当常见的攻击类型。

网络钓鱼是金融服务行业最常见的感染媒介，2021 年，该行业 46% 的攻击都是由网络钓鱼所导致的。漏洞利用排在第二位，它所导致的攻击在该行业遭受的攻击中占到了 31%。我们还发现，密码喷洒、暴力破解和 VPN 访问也是威胁实施者藉以对金融和保险公司发起攻击的感染媒介。

2021 年，亚洲的金融和保险组织遭到了大量攻击，占该行业所遭受攻击总量的 34%。中东和非洲的金融和保险组织遭受的攻击也非常之多，达到了 29%，而欧洲 (19%)、北美 (9%) 和拉丁美洲 (9%) 的金融和保险组织在 2021 年遭受的攻击所占比重则较小。

#3 | 专业与商业服务

专业服务涉及信息技术提供商、律师事务所、建筑师、会计师和专家顾问。商业服务则包括办公室管理、人力资源、安全服务、旅行安排和景观美化等公司。它们共同构成了一个更庞大的服务行业，我们正在将其纳入 2022 年 X-Force 威胁情报指数的考量范畴。

在 2022 年的攻击排行榜上，专业和商业服务公司位列第三，占所观察到的攻击总量的 12.7%。其中，24% 是商业服务公司，76% 是专业服务公司，29% 是专门以信息技术为重点的专业服务提供商。

勒索软件攻击是 2021 年专业和商业服务公司遭受的最主要攻击类型，占 X-Force 在这些行业观察到的攻击总量的 32%。服务器访问攻击是第二常见的攻击类型（19%），2021 年第四季度服务器访问攻击的增加与第四季度勒索软件攻击的减少正好吻合，这表明专业服务公司可以更好地及早识别和阻止勒索软件攻击者，让他们的目标落空。在对专业和商业服务行业发起的所有攻击中，恶意内部人员发起的攻击位列第三，占到了 13%。

2021 年，在 X-Force 对专业和商业服务公司实施补救的事件中，漏洞利用占到了 50%，网络钓鱼则占 20%。使用被盗凭证，也在我们对该行业实施补救的事件中占到了 20%。在多起漏洞利用事件中，威胁实施者都利用了 2021 年初披露的 Microsoft Exchange 漏洞。

占攻击总量的 12.7%

#4 | 能源

在今年遭受攻击最多的行业排行榜上，能源行业位列第四，在观察到的攻击总量中占到了 8.2%，从前一年的第三位下滑一位。在 DarkSide 于 2021 年 5 月对 Colonial Pipeline 发起的勒索软件攻击遭到反击之后，因害怕受到报复，威胁实施者（尤其是勒索软件实施者）可能已将注意力从能源组织转移。2021 年，X-Force 在 6 月、7 月和 8 月观察到的对能源组织发起的攻击事件都少于 5 月（Colonial Pipeline 于当月遭到了勒索软件攻击）。然而，到了 9 月，攻击量似乎再次回升。

占攻击总量的 8.2%

勒索软件攻击 (25%) 是 2021 年能源组织遭受的最常见攻击类型，其次就是 RAT、DDoS 和 BEC，它们并列第二 (17%)。僵尸网络、垃圾邮件和数据盗窃也在 2021 年对能源公司产生了一定的影响。

网络钓鱼是威胁实施者用于访问能源组织网络的最常见感染媒介，约占攻击总量的 60%，而漏洞利用则占剩下的 40%。

北美地区的能源组织遭受的攻击多于其他任何地区，在去年 X-Force 发现的所有针对能源行业的攻击中占到了 31%，接下来欧洲占 28%，拉丁美洲、中东和非洲以 17% 的占比并列第三，亚洲则以 7% 的占比居于末位。

#5 | 零售与批发

零售商店主要是将制成品直接销售给消费者，而批发组织则主要是直接通过制造商来分销和运输商品，通常是分销给第三方或直接出售给消费者。这些行业在 X-Force 2022 年遭受攻击最多行业榜单中排名第五，占 2021 年攻击总量的 7.3%。其中，35% 的攻击针对的是零售企业，65% 则将矛头直指批发企业，这凸显了威胁实施者去年对批发组织高度重视，这可能是由于它们在供应链以及商品从制造商到最终用户手中的流动过程中所发挥的关键作用。

占攻击总量的 7.3%

BEC、服务器访问、数据盗窃和凭证收集是去年零售和批发行业遭受的主要攻击类型。勒索软件和银行木马在攻击中所占的比重也很大，其次就是 RAT、配置错误和欺诈行为。

网络钓鱼是 2021 年威胁实施者藉以对零售和批发行业发起攻击的最主要感染媒介，在 X-Force 在该行业修复的已知初始感染媒介的攻击中占到了 38%。被盗凭证以 31% 的占比位居第二，漏洞利用在这些行业遭受的攻击中占到了 23%。暴力破解（8%）也在一些攻击中发挥了作用。

在 2021 年零售和批发行业遭受的攻击事件中，北美和拉丁美洲并列第一，各占 35%，而欧洲则紧随其后，为 31%。

#6 | 医疗保健

医疗保健行业在今年遭受攻击最多行业榜单中位列第六，占 X-Force 在 2021 年观察到的攻击总量的 5.1%，已从上一年的第七位上升一位。在医疗保健行业遭受的已知攻击类型的攻击中，38% 是勒索软件攻击，这一比例高于其他大多数行业。AtomSilo、AvosLocker 和 REvil 勒索软件实施者今年都将攻击的矛头指向了医疗保健组织。除了勒索软件攻击，今年 BEC 攻击 (25%) 也对医疗保健行业造成了相当严重的打击，服务器访问、凭证收集和配置错误也产生了一定的影响。

占攻击总量的 5.1%

漏洞利用是 2021 年威胁实施者藉以对医疗保健组织发起攻击的最主要感染媒介，X-Force 修复的事件中 57% 都是由漏洞利用导致的，其次就是网络钓鱼，占比为 29%，使用被盗凭证则占 14%。

中东和非洲的医疗保健组织在 2021 年遭受的攻击最多，占医疗保健行业所遭受攻击总量的 39%，紧随其后的是北美，占 33%。亚洲和拉丁美洲均占 11%，而欧洲仅占 6%。

#7 | 交通运输

交通运输行业遭受的攻击占攻击总量的 4.0%，从 2020 年的第 9 位上升至第 7 位。随着 2021 年国际边界和运输网络重新开放，该行业的活跃可能会再度吸引攻击者的兴趣。

恶意内部人员攻击成为 2021 年交通组织遭受的最主要攻击类型，占该行业攻击总量的 29%。勒索软件、RAT、数据盗窃、凭证收集和服务器访问攻击也都在 2021 年对交通运输行业产生了一定的影响。

在 2021 年 X-Force 对运输组织实施补救的所有事件中，有一半的事件起初是由网络钓鱼电子邮件引发的，其次便是使用被盗凭证，占到了 33%，漏洞利用所占比重则为 17%。

迄今为止，交通运输行业遭受的攻击大都集中在亚洲地区，占 2021 年 X-Force 观察到的该行业事件总量的 64%，其次便是欧洲 (21%)、中东和非洲 (7%) 以及北美 (7%)。

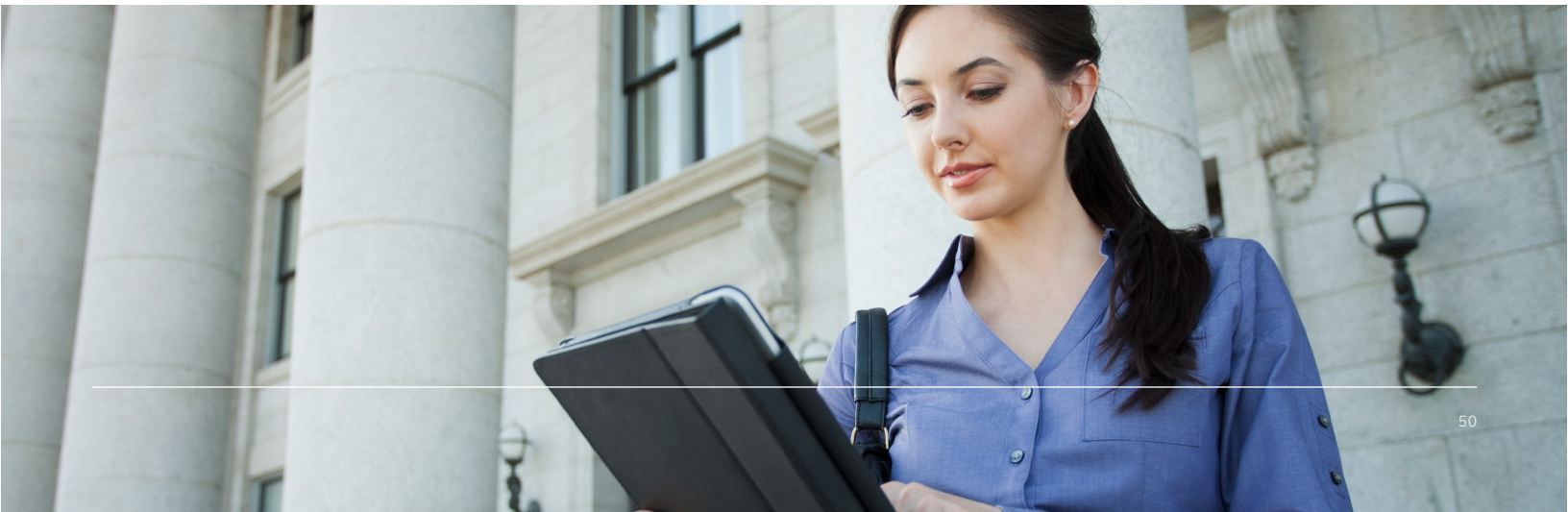
占攻击总量的 4.0%

#8 | 政府

在 2021 年，政府和教育行业在遭受攻击最多行业榜单上并列第八，占攻击总量的 2.8%。服务器访问攻击是去年对公共部门发起攻击的最常见攻击类型，这表明 2021 年 X-Force 的政府客户特别擅长于及早识别并根除网络中的威胁行为者，避免他们越过服务器访问生出更多枝节。数据盗窃和欺诈行为在 2021 年也跻身于政府遭受的三大攻击类型之列。漏洞利用是威胁实施者藉以对政府发起攻击的最常用的感染媒介，其次是网络钓鱼。

遭受攻击的政府在地理上分布广泛，其中有一半的攻击发生在亚洲，紧随其后的是北美，占比为 30%。中东和非洲 (10%) 以及欧洲 (10%) 也出现了一些针对政府组织的攻击行为。

占攻击总量的 2.8%



#9 | 教育

根据 X-Force 的研究，教育机构在 2021 年遭受的攻击占攻击总量的 2.8%，因此与政府部门并列第八。广告软件是 2021 年观察到的教育机构最常遭受的攻击类型，占攻击总量的 33%，紧随其后的是勒索软件，占 22%。去年，BEC、RAT、服务器访问攻击和欺诈行为在教育机构内也很常见。

网络钓鱼是威胁实施者藉以对教育行业发起攻击的最主要感染媒介，其次是暴力破解攻击。就 2021 年教育机构遭受的攻击事件而言，亚洲是攻击的重灾区，其次就是北美洲。

占攻击总量的 2.8%

#10 | 媒体

包括电信、新闻媒体、出版和电影制作在内的媒体行业在 2021 年遭受的攻击占攻击总量的 2.5%，跻身于遭受攻击最多的十大行业之列。勒索软件是所观察到的媒体机构遭受的最主要攻击类型，占 X-Force 在该领域观察到的攻击总量的 33%，其次是服务器访问、RAT、加密挖掘和恶意内部人员事件。暴力破解和被盗凭证是 X-Force 观察到的攻击者用来破坏媒体机构的主要方法，这表明该行业可能通过稳健实施 MFA 将若干种攻击类型挡在门外。媒体行业遭受攻击最严重的地区是欧洲和拉丁美洲，中东和非洲、北美以及亚洲也发生过针对媒体的攻击行为。

占攻击总量的 2.5%

风险缓解建议

我们在本报告中介绍的威胁可能会引起读者的担忧，因为本报告重点说明了来自勒索软件不断加剧的严重威胁、商业电子邮件攻击 (BEC) 和网络钓鱼攻击带来的新威胁，并强调了在去年一整年中，一些零日漏洞一直在被威胁实施者利用。但是，我们发布这份报告的目的是让组织更好地了解目前的威胁形势，帮助他们建立信心，采取所需的行动对抗这些威胁。

X-Force 发现，某些安全原则有助于对抗目前的网络威胁，这包括零信任方法、安全事件响应自动化以及扩展的检测和响应能力。

零信任有助于降低最主要攻击的风险

零信任是行为模式的转变，是解决安全问题的新方法，它假设安全违规已经发生，旨在加大攻击活动渗透到整个网络的难度。其核心理念是了解关键数据位于何处，以及谁有权访问这些数据，它在整个网络中建立强有力的验证措施，以确保只有具有权限的个人才能以适当的方式访问这些数据。

X-Force 威胁研究人员的研究证实，与零信任方法相关的原则（包括实施 MFA 以及最少特权原则）有助于降低组织对本报告中确定的最主要攻击类型的脆弱性，特别是勒索软件和 BEC。

尤其是，通过将最少特权原则应用于域控制者和域管理员帐户，可以增加勒索软件攻击者所面临的障碍，因为许多攻击者都是通过被破解的域控制者帐户向网络部署勒索软件的。此外，实施 MFA 会增加网络犯罪分子接管帐户的难度，因为这会要求他们提供进一步的认证，仅仅盗取凭证无法攻破网络。

了解有关如何建立零信任方法的更多信息

安全自动化增强事件响应能力

X-Force 安全事件响应工作团队每年都要处理不同地理区域中的数百起安全事件，协助内部安全事件响应分析员，解决一系列范围广泛的攻击类型。速度是关键，无论是在威胁实施者在网络上部署勒索软件之前发现并消灭他们，还是快速高效地解决问题，以便为处理下一次安全事件赢得时间。在这个快节奏的环境中，安全自动化是关键 - 将会占用分析人员或团队时间的机器任务外包出去，并确定改进工作流程的机制。

在 2021 年年中，IBM 向"开放网络安全联盟"(Open Cybersecurity Alliance) 捐赠了一个威胁搜寻自动化工具，旨在协助安全运营中心 (SOC) 分析师快速开展取证调查，解决网络安全事件。此外，X-Force IR 团队使用 IBM Security QRadar SOAR 增强其安全事件响应能力。

了解有关 IBM 安全事件响应服务的更多信息

扩展的检测和响应能力帮助我们针对攻击者形成巨大优势

通过使用检测和响应技术，尤其是将几种不同的解决方案合并为一个扩展的检测和响应 (XDR) 解决方案，为组织带来了显著的优势，能够在攻击者到达最终攻击阶段（例如勒索软件部署或数据盗窃）之前发现和根除他们。

在多个例子中，当 X-Force IR 团队在客户的网络上部署终端检测和响应 (EDR) 或 XDR 解决方案后，IR 能够立即获得额外的洞察，这有助于发现并快速应对攻击者的活动。XDR 技术有助于更有效地防御 X-Force 观察到的服务器访问和其他攻击类型，这表明攻击者在达到目的之前就被发现和阻止。

了解有关 IBM Security QRadar XDR 的更多信息。

建议

以下建议包含组织可采取的具体措施，以便更有效地保护网络的安全，防止本报告中分析的威胁。

针对勒索软件制定响应计划。所有行业和所有地理地域都处于勒索软件攻击的风险之中，团队应对关键时刻的方式会对所花时间和经济损失产生显著影响。

- 在响应计划中包含要立即采取的限制措施、应告知利益相关方和执法部门官员的内容、组织安全地进行存储并从备份中恢复的方法，以及在修复期间运行关键业务职能的备用地点。
- 在计划中包含勒索软件攻击过程中的数据盗窃和泄露场景 - 这些场景是勒索软件目前非常常见的策略，在 X-Force 修复的勒索软件攻击中的出镜率非常高。
- 进行勒索软件攻防演练，充分考虑组织是否会支付赎金，以及哪些因素会改变对该决策的考量。
- 确保勒索软件响应计划包含与云相关的安全事件的特定应急方案，因为这可能需要额外的工具和技能。
- 使用闪存解决方案，避免因恶意软件或勒索软件攻击而造成数据损坏，闪存解决方案有助于防止数据丢失、促进运营连续性，以及降低基础架构成本。
- X-Force 的《勒索软件权威指南》就如何应对勒索软件攻击提供了更多详细的建议。X-Force 的安全事件响应团队还可以为贵组织开展勒索软件准备情况评估，帮助制定和检验勒索软件事件响应计划。与此类似，X-Force 指挥中心也可以帮助组织为勒索软件攻击做好应对准备，同时考虑所需的业务和技术应对措施。

对每个远程网络访问点实施多因子认证。X-Force 发现，越来越多的组织比以往更成功地实施 MFA。这实际上改变了威胁态势，迫使威胁实施者寻找新的网络入侵方式，仅仅利用被盗的电子邮件凭证无法攻破防线；此外，还降低了电子邮件接管攻击活动的有效性。

- MFA 有助于降低多种不同的攻击类型的风险，包括勒索软件、数据盗窃、BEC 和服务器访问等。
- 此外，身份和访问管理技术使 MFA 实施每年都变得更简单，无论是对于实施团队还是最终用户而言。

采用分层方法对抗网络钓鱼攻击。遗憾的是，目前没有任何一种工具或解决方案可以阻止所有网络钓鱼攻击，威胁实施者持续优化社会工程攻击和反恶意软件检测方法，以规避既有的安全控制机制。因此，我们建议实施多层解决方案，以提高捕获网络钓鱼电子邮件的机会。

- 首先，有效提高用户的安全意识和安全培训水平，并为他们提供现实世界的示例。
- 其次，采用电子邮件软件安全解决方案，让机器担负起发现和过滤恶意电子邮件的任务。
- 第三，实施多道防线，帮助捕获恶意软件或者内网漫游，防止网络钓鱼电子邮件快速溜过，这包括基于行为的反恶意软件检测、终端检测和响应 (EDR)、入侵检测和预防解决方案 (IDPS)，以及安全信息和事件管理 (SIEM) 系统。

确保漏洞管理系统不断完善，日臻成熟。漏洞管理是一门艺术 - 这包括确定哪些漏洞最适合贵组织的网络架构，以及确定如何在不影响流程中任何内容的情况下部署该系统。

- 建立一个专门负责漏洞管理的团队，为该团队提供充足的资源和支持，从而确保贵组织的网络受到严格保护，远离潜在的漏洞利用攻击。
- 我们建议优先考虑此评估中提到的适用于贵组织的任何漏洞。
- IBM 的 X-Force Exchange 还包含漏洞和相关严重性级别的存储库，可帮助您发现最关注的漏洞；此外，X-Force Red 可提供专门的漏洞扫描和管理服务。

关于 IBM Security X-Force

IBM Security X-Force 是以威胁为中心的团队，由黑客、应对人员、研究人员和分析人员组成。我们的产品服务组合包括各种进攻性和防御性的产品和服务，以全方位的威胁情报提供支持。通过与 X-Force 合作，您可以确信自己面临的数据泄露风险的发生可能性和影响降到最低。

IBM Security X-Force 威胁情报结合了 IBM 安全运营遥测、研究、事件响应调查、商业数据和开放资源，可帮助客户了解新出现的威胁并快速做出明智的安全决策。

此外，X-Force 事件响应团队提供检测、响应、修复和准备服务，帮助您最大程度降低数据泄露的影响。

X-Force 结合 IBM Security 指挥中心的丰富经验，培训您的团队（从分析人员一直到最高管理层），帮助他们为目前的威胁现实状况做好准备。X-Force Red 是 IBM Security 的黑客团队，负责提供进攻性安全服务，包括渗透测试、漏洞管理和对手模拟等。

这一年来，IBM X-Force 研究人员还以博客、白皮书、网络研讨会和播客等形式提供了持续性的研究和分析，重点强调了我们在高级威胁实施者、新恶意软件和新攻击方法方面的洞察力。此外，我们在整个 X-Force 威胁情报解决方案中为订阅客户提供了大量最新的前沿分析。

了解有关 IBM Security QRadar XDR 的更多信息。

关于 IBM Security

IBM Security 竭诚与您合作，帮助您保护企业安全，为您提供融合了 AI 技术以及采用零信任原则的现代安全战略方法的高级集成式企业安全产品与服务组合，支持贵组织在充满不确定性的世界里蓬勃发展。我们的集成式解决方案能够使您的安全策略与您的业务保持一致，旨在保护您的数字用户、资产和数据，帮助您通过部署技术来管控和抵御日益增长的威胁。此外，我们还会帮助您管理和治理支持当今混合云环境的风险。

我们全新的现代开放式方法 IBM Cloud Pak for Security 基于 RedHat Open Shift，旨在利用广泛的合作伙伴生态系统支持当今的混合多云环境。Cloud Pak for Security 是面向企业的容器化软件解决方案，通过快速集成现有的安全工具，深入洞察混合云环境中的威胁，从而帮助您轻松管理数据和应用的安全性 - 数据都保留在原处，轻松实现安全响应统筹和自动化。

如需了解更多信息，请访问 www.ibm.com/cn-zh/security 或阅读 IBM 安全情报博客。

贡献者

Camille Singleton
Charles DeBeck
Joshua Chung
Dave McMillen
Scott Craig
Scott Moore
Charlotte Hammond
John Dwyer
Melissa Frydrych
Ole Villadsen
Richard Emerson
Guy-Vincent Jourdan
Vio Onut
Stephanie Carruthers
Adam Laurie
Michelle Alvarez
Salina Wuttke
Georgia Prassinos
John Zorabedian
Mitch Mayne
Limor Kessem
Ian Gallagher
Ari Eitan

国际商业机器中国有限公司
北京市朝阳区北四环中路27号
盘古大观写字楼25层
邮编: 100101

美国出品
2022 年 2 月