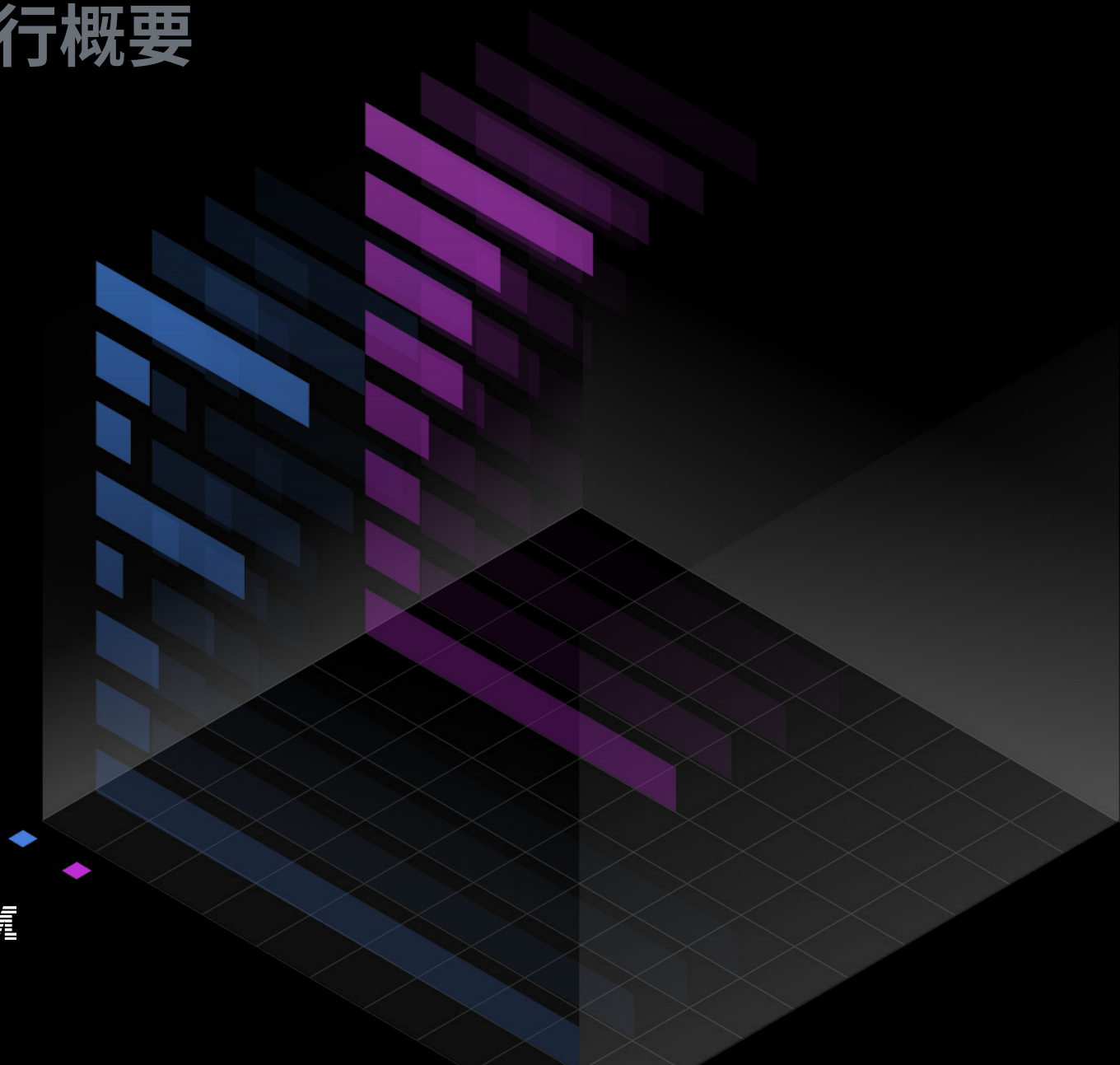
IBM Security

X-Force 威胁情报指数 2021

执行概要



IBM

简介

毫无疑问，2020 年是我们最近记忆中最重要、最具变革性的一年：新冠疫情肆虐，经济动荡影响着数百万人的生活，还有社会和政治动荡。这些事件的回响对企业产生了深远的影响，许多企业开始向分布式劳动力大举转移。

在网络领域，2020 年的特殊情况使得网络攻击者有机会利用我们所必需的通信网络实施攻击，同时供应链和关键基础架构中也为网络攻击者提供了丰富的目标。一年的时间稍瞬即逝，我们发现了一种席卷全球的重大威胁，而这需要我们迅速做出响应并采取补救措施。该威胁在很大程度上归因于某个民族国家威胁实施者的攻击，利用网络监控软件中的后门攻击政府和私营部门组织，这表明第三方风险应该被预测，但却无法预测。

为了帮助各种组织应对当今时代的挑战，IBM Security X-Force 对网络威胁格局进行了评估，并帮助组织了解不断演变的威胁、与之相关的风险以及如何对网络安全工作进行优先排序。除了为客户提供优质威胁情报之外，我们还对收集到的大量数据进行了分析，进而编制了“X-Force 威胁情报指数报告”- 关于威胁格局及其变化情况的年度检查报告。

在我们追踪的趋势中，勒索软件攻击继续呈上升趋势，是第一大威胁类型，在 X-Force 2020 年所响应安全事件中的占比为 23%。勒索软件攻击者通过结合采用数据加密及公共站点上的数据泄露威胁，加大了勒索付款的压力。根据 X-Force 的估算，这些阴谋的成功，让一个勒索软件团伙在 2020 年获得了超过 1.23 亿美元的利润[1]。

制造业组织在 2020 年遭受了勒索软件和其他威胁类型的猛烈攻击。总体而言，制造业成为第二大被攻击者所针对的行业，仅次于金融与保险业，而在 2019 年，制造业在这方面的排名才只有第八位 X-Force 发现了一些高级攻击者使用针对性鱼叉式钓鱼活动，专门攻击参与 COVID-19 疫苗供应链的制造企业和非政府组织。

威胁实施者也在创新他们的恶意软件，特别是针对 Linux 的恶意软件，而 Linux 是一种支持业务关键云基础架构和数据存储的开源代码。Intezer 的相关分析显示，在 2020 年共发现了 56 个新的 Linux 恶意软件系列，远远超过其他威胁类型的创新水平。

我们有理由希望 2021 年会成为更好的一年。众所周知，趋势很难预测，但是我们可依赖的唯一不变就是“改变”本身。面对日益严峻的网络安全挑战，若要确保弹性，就需要可执行的情报和战略愿景，实现更开放、更互联的安全性。

1. 本报告中的所有货币均为美元。

本着希望通过社区增强安全理念的精神，IBM Security 发布了 2021 年 X-Force 威胁情报指数报告。本报告中的调查结果可以帮助安全团队、风险专业人士、决策者、研究人员、媒体和其他人员了解过去一年来的威胁，并为接下来的事情做准备。

执行概要

IBM Security X-Force 利用在 2020 年 1 月至 12 月期间从我们的客户和公共来源收集的数十亿数据点来分析攻击类型、感染媒介以及全球和行业比较。以下是 X-Force 威胁情报指数中列出的一些主要发现。

23%

勒索软件在攻击事件中所占的比例

勒索软件是 2020 年最流行的攻击类型，在 IBM Security X-Force 响应并帮助补救的所有事件中占比 23%。

超过 1.23 亿美元

攻击者通过主要勒索软件所得利润

X-Force 保守估计，Sodinokibi（也称为 REvil）勒索软件攻击实施者在 2020 年至少获利 1.23 亿美元，窃取了约 21.6 TB 的数据。

25%

2020 年第一季度攻击者所利用的最大漏洞所占的比例

威胁实施者利用路径遍历 Citrix 漏洞开展了许多攻击，利用该漏洞实施的攻击在 2020 年前三个月的攻击中所占的比例为 25%，在 2020 年所有攻击中所占比例为 8%。

35%

扫描和漏洞利用在主要入侵媒介中所占比例

扫描和漏洞利用在 2020 年超过钓鱼攻击（2019 年占比最高的入侵媒介），跃升为占比最高的入侵媒介

#2

制造业在受攻击最严重行业中的排名

制造业是 2020 年遭受攻击次数第二多的行业，仅次于金融服务业，而在 2019 年，制造业位列第八。

5 小时

在威胁实施团伙服务器上发现的攻击培训视频的时长

由于伊朗民族国家攻击者的操作失误，X-Force 研究人员在他们配置错误的服务器上发现了时长大约 5 个小时的视频，进而深入了解了他们的技术。

100+

某场精准钓鱼攻击活动中被针对的高管人员数量

2020 年中，X-Force 发现了一场全球性钓鱼攻击活动，该活动的攻击对象是 100 多名担任采购和管理角色的高管人员，他们所在工作小组的任务是采购用于对抗新冠疫情的个人防护设备 (PPE)。

49%

2019-2020 年 ICS 相关漏洞数量的增长率

与 2019 年相比，2020 年发现的工业控制系统 (ICS) 相关漏洞数量同比增长了 49%。

56 个

新的 Linux 恶意软件家族数量

2020 年，新发现的与 linux 相关的恶意软件家族数量为 56 个，是有史以来的最高水平。从 2019 年到 2020 年同比增长 40%。

31%

欧洲攻击所占份额

根据 X-Force 的观察，欧洲是 2020 年遭受攻击最多的地区，
经历了 31% 的攻击，其次是北美 (27%) 和亚洲 (25%)。

展望未来

2021 年，新老威胁交织在一起，需要安全团队同时考虑许多风险。根据 X-Force 分析，以下是明年优先考虑的一些关键事项。

- **风险面将在 2021 年继续增长。**新旧应用程序和设备中都可能报告数千个新的漏洞。
- **勒索软件的双重勒索可能会持续到 2021 年。**攻击者在名称和耻辱站点上公开泄漏数据，提高了威胁主体利用勒索软件感染索要高价的筹码。
- **威胁主体继续将目光投向不同的攻击媒介。**Linux 系统、运营技术 (OT)、物联网设备和云环境将继续成为攻击的目标。随着这些系统和设备的目标变得更加先进，威胁主体可能会迅速调整攻击力度，特别是在发生任何重大事件之后。
- **每个行业都面临各自的风险。**行业特定目标的逐年变化凸显了所有行业部门面临的风险，也凸显了全面推进和成熟网络安全计划的必要性。

弹性建议

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/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，才能在变化莫测的环境里规避威胁。

X-Force 建议组织采取以下措施，以便在 2021 年更好地应对网络威胁：

走在威胁的前面，而不是被动应对。利用威胁情报，以更好地了解威胁主体的动机和策略，从而对安全资源进行优先级排序。

做好准备是应对勒索软件的关键。为勒索软件攻击制定计划（包括解决混合勒索软件和数据盗窃勒索技术的计划），并定期演练该计划，可以使您的组织在关键时刻做出完全不同的反应。

仔细检查组织的补丁程序管理结构。鉴于扫描和利用是去年最常见的感染媒介，加强您的基础架构并重新激活内部检测能力，以快速有效地发现并阻止自动利用尝试。

防范内部威胁。使用数据丢失防护（DLP）解决方案、培训和监控来防止无意或恶意的内部人员破坏您的组织。

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。

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漏也能降低损失。

实施多因素身份验证 (MFA)。为帐户添加保护层仍然是组织最有效的安全优先事项之一。

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，特别是在 2020 年数据显示勒索软件活动重新抬头的情况下。

关于 IBM Security X-Force

IBM Security X-Force 提供洞察、检测和响应能力，以帮助客户改善安全状况。

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，训练有素的 X-Force 事件响应团队提供战略补救措施，以帮助组织更好地控制安全事件和违规行为。

X-Force 结合了 IBM 安全指挥中心的网络靶场经验，培训客户为应对当今的威胁做好准备。

全年中，IBM X-Force 研究人员还以博客、白皮书、网络研讨会和播客的形式提供持续的研究和分析，强调我们对高级威胁主体、新的恶意软件和新的攻击方法的洞察力。此外，我们还通过高级威胁情报平台为订阅客户提供大量最新的前沿分析。

后续行动

详细了解有关与 IBM Security 协调开展事件响应的信息 >

关于 IBM Security

IBM Security 与您全力合作，通过融合了 AI 的先进、集成式企业安全产品和服务组合，以及采用零信任原则的现代安全策略方法来保护您的业务，从而帮助您在不确定的情况下蓬勃发展。通过使安全策略与业务保持一致；集成旨在保护您的数字用户、资产和数据的解决方案；并部署技术来管理针对日益增长的威胁的防御，我们将帮助您管理和治理支持当今混合云环境的风险。

我们新的现代开放式方法 IBM Cloud Pak for Security 平台基于 RedHat Open Shift 构建，并通过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 是一种企业就绪的容器化软件解决方案，通过快速集成您现有的安全工具，对混合云环境中的威胁产生更深入的洞察，从而使您能够管理数据和应用程序的安全性，将数据保留在原处，轻松编排和自动化您的安全响应。

如需了解更多信息，请浏览 www.ibm.com/security、在 Twitter 上关注 @IBMSecurity或访问 IBM 安全情报博客。

合作者

首席作者：
Camille Singleton

合作者： Allison Wikoff
Ari Eitan (Intezer)
Charles DeBeck
Charlotte Hammond
Chenta Lee
Chris Sperry
Christopher Kiefer
Claire Zaboeva
David McMillen
David Moulton
Dirk Hartz
Georgia Prassinos
Ian Gallagher (Intezer)
John Zorabedian
Joshua Chung
Kelly Kane
Lauren Jensen
Limor Kessem
Mark Usher
Martin Steigemann
Matthew DeFir
Megan Radogna
Melissa Frydrych
Michelle Alvarez
Mitch Mayne
Nick Rossman
Patty Cahill-Ingraham
Randall Rossi
Richard Emerson
Salina Wuttke
Scott Craig
Scott Moore

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
2021 年 2 月