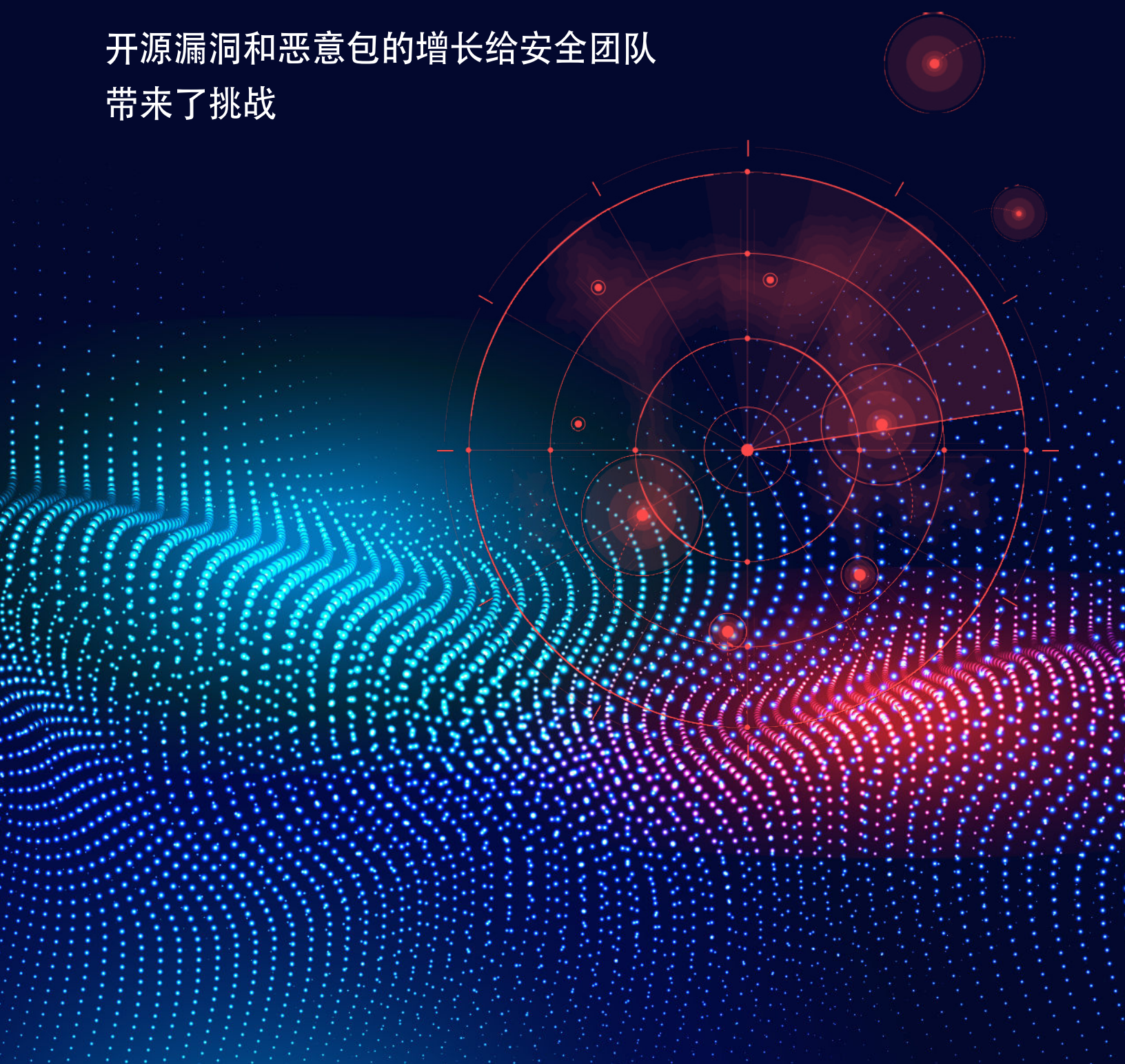
MEND itbigtec 艾体宝

Mend 开源风险报告

开源漏洞和恶意包的增长给安全团队带来了挑战



摘要：

Mend在2022年前9个月识别并添加到其漏洞数据库中的恶意软件包数量比2021年前9个月增加了33%，反映了已发布的开源软件包数量的增长和漏洞的加速。与此同时，许多公司都在努力缩小补救差距。虽然公司每月修复数千个漏洞，但需要现代最佳实践才能跟上每月检测到的新漏洞浪潮。

71% 的 IT 和安全领导者表示，他们的应用程序组合更容易受到攻击。现在，又有 70% 至 90% 的应用程序使用了开放源代码。显然，开放源代码漏洞的不断增加给严重依赖应用程序取得成功的企业带来了巨大风险。

漏洞更多、更复杂、更不清晰

不幸的是，这给黑客带来了一些可利用的机会，他们总是很快地利用新材料。通过利用增加的漏洞缓存来发起利用多个漏洞的攻击，攻击者可以成倍地增强他们的武器库，并针对公司难以修复的缺陷。这也凸显了仅遵守CVD分数作为衡量漏洞危险程度的不足。有效的优先顺序不仅需要严重性细节，还需要有关如何单独利用特定缺陷以及与其他缺陷结合利用的背景。

日益增长的挑战：恶意包

我们看到2022年发布的恶意软件包数量稳步增加，第三季度大幅增加，较第二季度增长了79%。每天至少有十个恶意包被发布到NPM和rubygems。攻击者还部署了更复杂的技术。更多的软件包包含能够进行数据收集的遥感技术，有些包隐藏得更深，例如有效内容具有包含恶意代码的依赖项。

关键发现：

- 与 2021 年同期相比，Mend 在 2022 年前九个月向其漏洞数据库添加的开源软件漏洞数量增长了 33%。这超过了开放源代码软件数量 25% 的增长速度。
- 根据 2022 年 1 月至 9 月对 900 多家公司进行的代表性抽样调查，发现只有 13% 的漏洞得到了修复，而使用repo集成的公司则有 40% 的漏洞得到了修复。
- Mend Supply Chain Defender 的数据显示，2022 年发布的恶意软件包数量按季度稳步增长，第三季度大幅跃升，比第二季度增加了 79%。

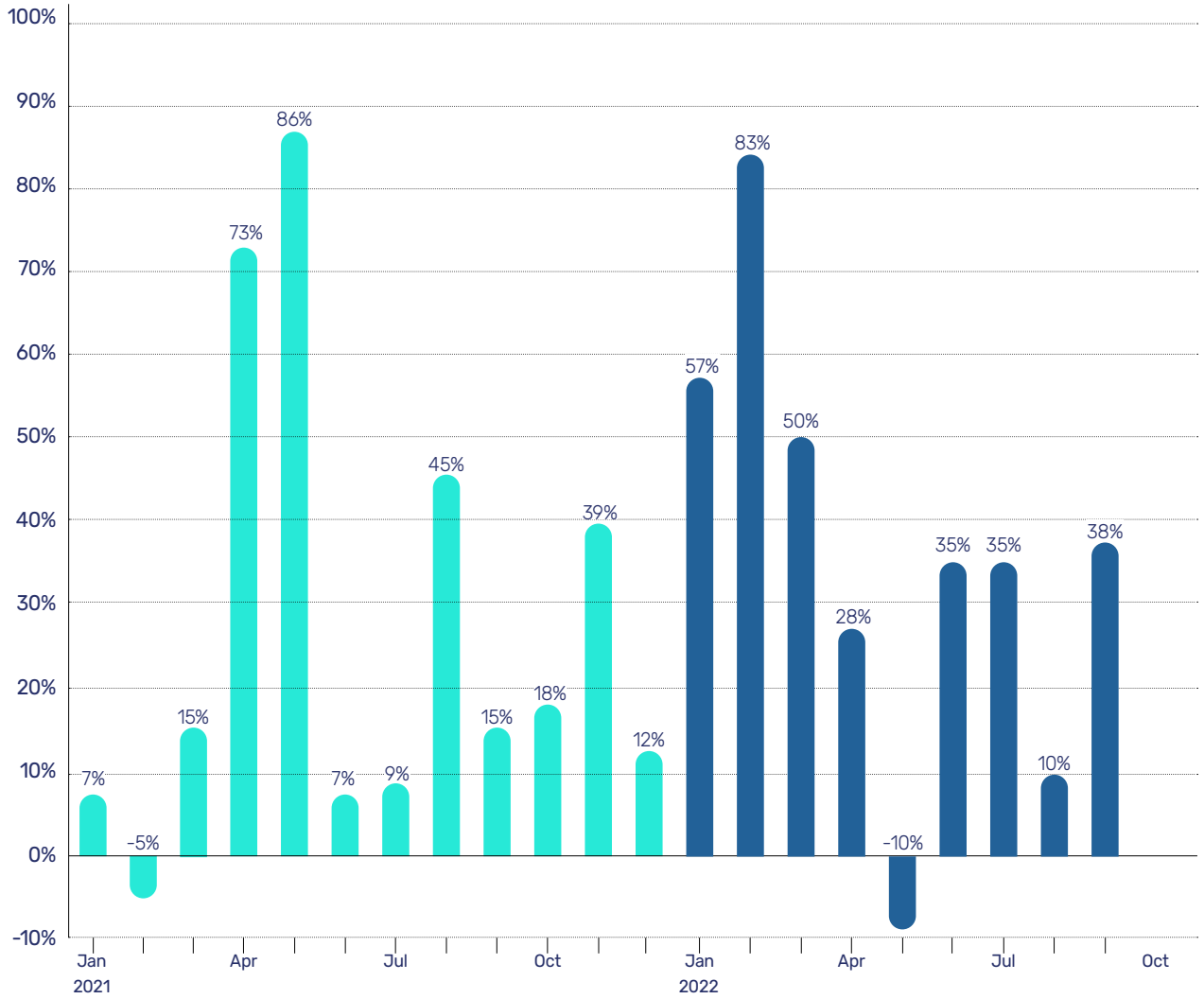
% 开源代码漏洞增长

开源代码漏洞趋势

总体增长

一般来说，Mend 漏洞数据库的数据显示，开源漏洞的增长速度相对保守，与开源软件日益普及的趋势基本吻合。例如，在 2021 年，Mend 添加到漏洞数据库的新开源漏洞数量比前一年增加了 25%，这与开源软件数量约 25% 的增长速度基本一致。但在 2022 年，截至 9 月份，我们看到开源漏洞的数量增加了 33%。

2021 年 1 月至 2022 年 9 月按月分列的开放源代码漏洞情况

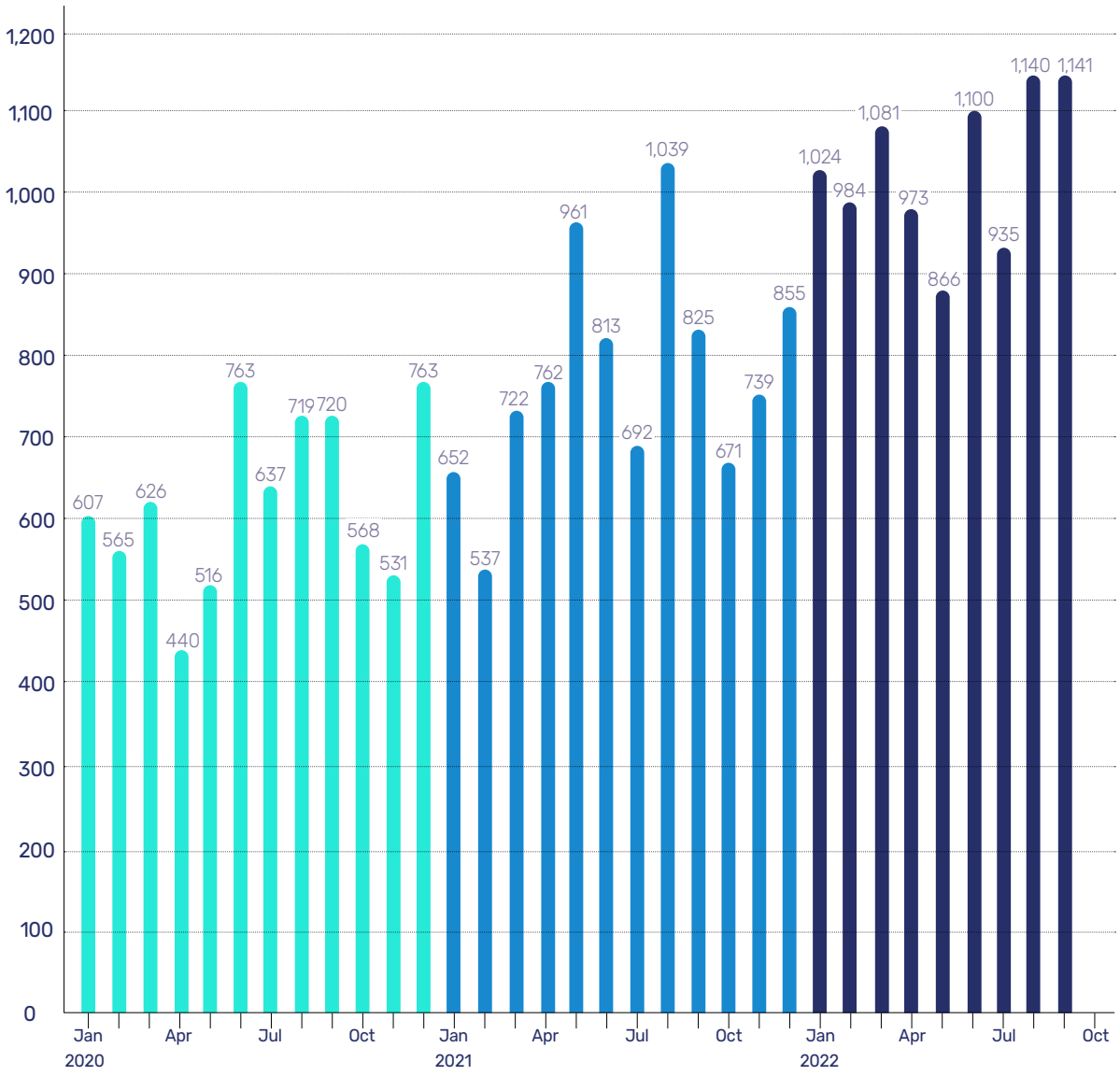


漏洞总数的增长意味着黑客可利用的原材料大幅增加，他们清楚地意识到应用程序和其他软件组件是一个很好的目标。更糟糕的是，这些漏洞所构成的威胁大于其各部分的总和。原因就在于：实际风险并不是由漏洞总数来表示的。而是这些漏洞被成功用于攻击的几率。如今，恶意行为者发起的攻击越来越复杂，其中包含多种漏洞。这意味着，随着可用漏洞数量的增加，利用多个漏洞成功发起攻击的几率也呈指数级增长。

此外，这也凸显了仅以 CVSS 分数来衡量漏洞危险程度的不足。例如，美国联邦调查局关于 APT10的简报中，列出了 APT10 在攻击中使用的大量 CVE。其中一半以上是低级和中级安全问题。这说明，基于严重性的“ 排序和响应 ”并不总是有效的。攻击者的复杂性已经淘汰了这种方法，因为中低级别的漏洞现在已经成为攻击的活跃部分。现在，防御者需要了解如何利用漏洞，以便有效地确定优先级。

持续增长模式

越来越多的开源代码被创造出来，而威胁行为者又有动力去寻找新的漏洞，这两者的结合几乎保证了开源漏洞不会在短期内减少。



来源：Mend漏洞数据库

为什么会出现这种跳跃式增长？2022 年迄今为止，已知开放源代码漏洞数量的增加有几种可能。

- 总体使用量增加。开放源代码软件的使用量不断扩大，我们的整个开发者社区也在不断扩大，更不用说可用的开放源代码数量的增加了。
- 与此同时，开放源码软件安全研究领域也呈上升趋势，从事该领域研究的公司和研究人员越来越多。此外，自动化也是今年发现大量漏洞的原因之一。安全研究人员正在使用自动扫描和检测工具来发现漏洞，使他们能够快速、大量地发现和修复安全问题。在某些情况下，研究人员发现了多个 CVE，一个共同的问题影响了许多项目。有时一个 CVE 适用于多个项目，但有时每个项目都有自己的 CVE 。
- CVE计划增加了CVE编号机构（CNA），这也是公布漏洞数量增加的原因之一。CNAs 由软件供应商、开源项目、协调中心、漏洞赏金服务提供商、托管服务和研究团体组成，经 CVE 计划授权，可为漏洞分配 CVE ID，并在各自特定的覆盖范围内发布 CVE报告。目前有来自 35 个国家的 251 个合作伙伴参与其中。
- 我们也不能忽视黑客群体的不懈努力。简而言之，随着OSS代码使用量的增加，我们不知道的漏洞增长的可能性也会增加。这为攻击者带来了更多的机会和更广泛的威胁格局。

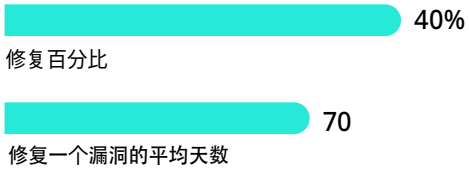
开源安全： 从用户角度看问题

我们希望从用户的角度审视开源安全。从 2022 年 1 月到 9 月，我们对北美约 1000 家不同行业、不同规模的公司进行了代表性抽样调查，整理出了有关关键漏洞、高严重性漏洞和修复情况的数据，为我们展示了开源安全现状的一个缩影--以及 Mend 所能带来的变化。

漏洞修复基线2022年1月~9

接下来，我们选取了一些具有代表性的公司样本，这些公司通过repo集成实施了 Mend 最佳实践。

集成repo的漏洞修复2022年1月~9月



结果很能说明问题。已修复漏洞的增加约等于风险降低了三倍，而修复时间缩短了 75%。

修复的差距

虽然公司每个月都会修复数千个漏洞，但许多公司仍积压着大量未修复的漏洞。为什么会出现这种情况？公司面临修复缺口的原因有很多：

缺乏时间和资源。应用安全团队往往工作过度、人手不足，这已不是什么秘密，这导致公司在决定对哪些应用打补丁并保持最新时，不得不做出艰难的决定。例如，有些公司只关注旗舰应用程序，认为不这样做的业务风险太高。

缺乏细化信息。虽然 CVE 严重性指数是一个合理的初始指标，可用于决定首先修复哪些漏洞，但仅靠它本身是不够的。对于应用程序安全团队来说，根据漏洞本身以及利用多个漏洞进行攻击时所造成的风险来识别漏洞并确定优先级至关重要。例如，许多漏洞在应用程序中并不构成风险，如果能够识别出来，就可以安全地忽略它们。这也意味着，中低严重性的漏洞也不容忽视，因为它们可以被用于多重漏洞攻击。

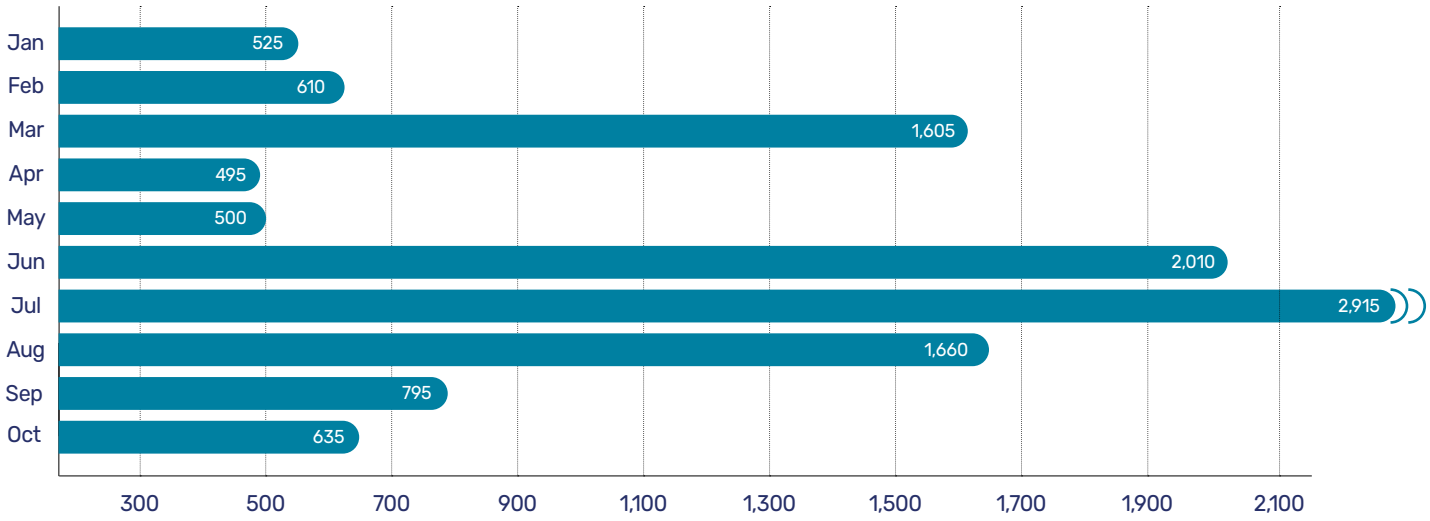
需要平衡安全风险和功能风险。虽然应用程序的安全性对业务应用程序至关重要，但保持其功能性也同样重要。在决定是否修补或升级用于构建应用程序的许多开源组件和相关依赖项时，这可能会带来棘手的问题。依赖项更新中的回归错误可能会导致生产问题，这种风险有多大？大多数团队无法投入大量工作来手动审查每个更新。相反，团队开始转向能够在不影响应用程序功能的情况下自动更新依赖项的工具。

恶意包

Mend的自动恶意软件检测平台Supply Chain Defender每月都会在nPM和rubygets中检测并报告数百个恶意软件包。从2022年1月到9月，我们看到2022年发布的恶意软件包数量每季度稳步增加，第二季度到第三季度增加了79%。每天至少有十个恶意包被发布到nPM和rubygems。

攻击者还部署了更复杂的技术。更多的包包含能够进行数据收集的遥感技术，有些包现在更深入地构建在软件供应链中，例如当有效内容具有包含恶意代码的依赖项时。攻击者还使用合法的托管提供商来发送恶意代码，而其他攻击者则隐藏在域名后面，建议合法的用例。我们在知名的加密货币交易所DyDx的攻击中看到了后一种方法。在DyDx的情况下，恶意包版本包含一个预安装Hook，使其看起来就像即将下载CircleCI脚本一样。这是最纯粹的品牌劫持-该域名看起来就像属于合法的CI/CD提供商。

2022年1月~10月，每月发布的恶意软件包数量



来源: Mend Supply Chain Defender

恶意软件包版本

恶意软件包平均有三个版本。我们发现一种趋势，即先发布非恶意版本，然后再发布恶意版本。这里有几个有趣的现象。与更新版本相比，首次发布的版本会进行初步清理。我们还看到版本发布反映了学习曲线。要制作一个具有高渗透概率的软件包是很难的，因此恶意行为者经常会在不同版本之间修补和调整他们的代码。

2022年1月-10月，每月发布的恶意版本

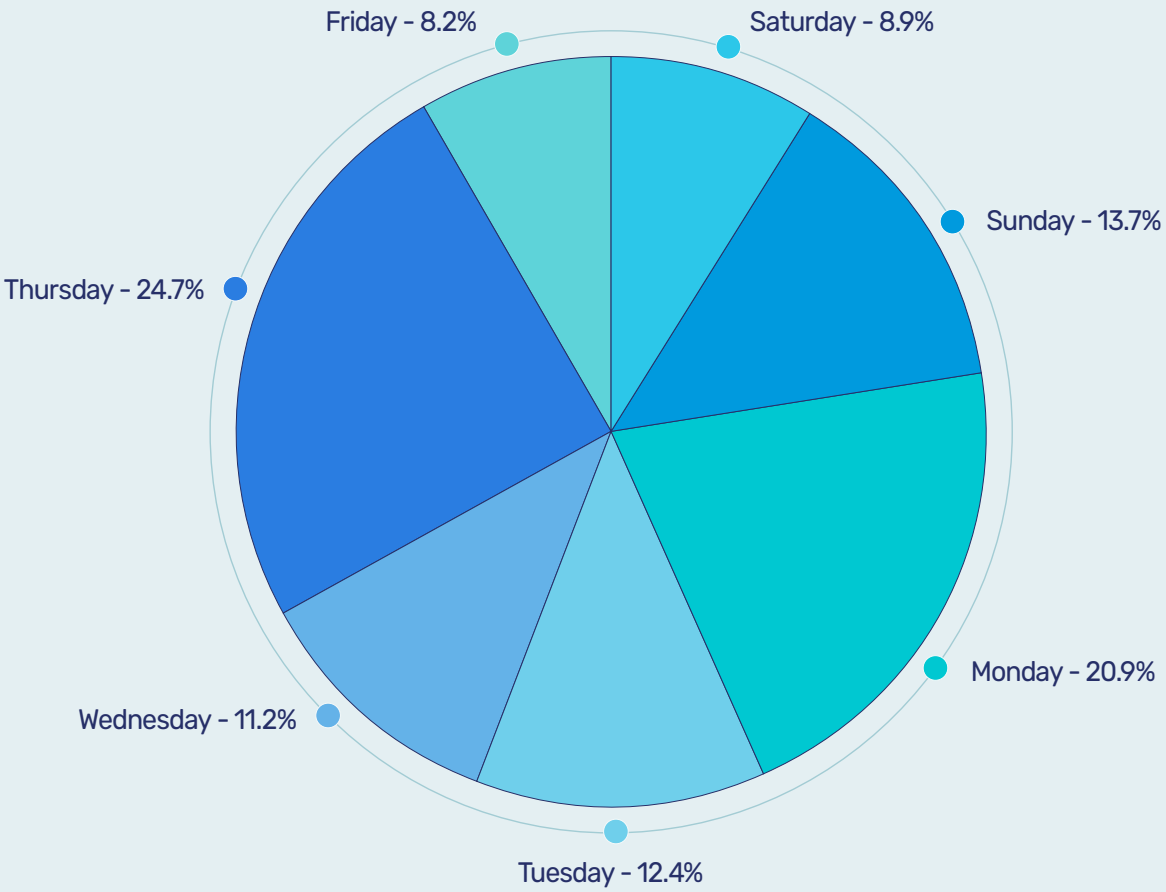
月份	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct
每月发布的恶意版本	1,835	2,210	4,087	6,097	1,914	4,651	6,198	6,729	2,535	1,925
每个包的恶意版本比例	3.5	3.6	2.5	12.3	3.8	2.3	2.1	4.1	3.2	3.0

攻击时机：没有意外

在我们的 2021 年报告中，攻击者最喜欢在周五、周六和周日（也称周末）发布恶意软件。我们将其解释为威胁行为者在安全研究人员最有可能错过的日子里发布软件包。大量的 npm 软件包和新软件包的发布速度使监控变得十分困难，而两天的数据积累可能会使问题更加严重。

今年，近25%的在周四下午发布。为什么会改变？越来越多的攻击者意识到，绝大多数网络安全公司都在以色列，因此他们寄希望于这样一个事实：那里的许多公司将周五和周六定为周末。将CET转换为以色列时区，我们看到攻击在下午4点左右开始。

恶意活动模式



来源：Mend supply chain defender
(本图的数据取自中欧时间CET.)

挖掘恶意软件历史记录以获取恶意软件包创新的线索

自 20 世纪 90 年代末首次出现恶意软件以来，恶意软件已经取得了很大的进步。如今，攻击者利用各种创新技术从世界各地的企业攫取大量资金。
类似的发展也出现在恶意软件的新兴“ 表亲 ”——恶意软件包的出现上，这些恶意软件包被上传到软件包注册库中。就像任何一个年轻的兄弟姐妹一样，恶意软件包还不像通用恶意软件那样成熟。我们观察到它们的发展大约落后了十年。这是可以理解的，因为恶意软件包代表了一种相对较新的机会和攻击面，网络犯罪分子才刚刚开始意识到它们的潜力。
恶意软件的历史也能提供有关未来恶意软件包趋势的重要线索。通过观察恶意软件在过去 20 年中的演变以及当前恶意软件包的发展趋势，我们可以预测恶意软件包未来可能的发展方向。主要有三个方面：攻击载体、恶意技术和目标。

攻击载体

恶意软件包有四种基本攻击载体：品牌劫持、typosquatting、依赖劫持和依赖混淆。

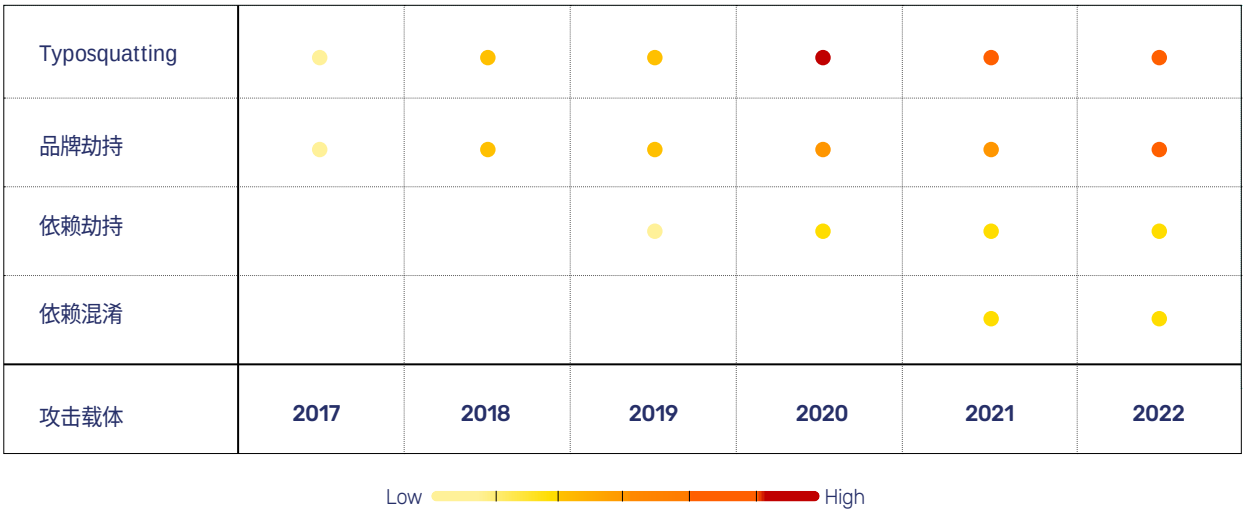
品牌劫持是指攻击者获取或以其他方式假冒其他公司或软件包所有者的在线身份，然后插入恶意代码的活动。这并不一定意味着他主动窃取了什么东西，而只是利用机会获取了与品牌名称相关的所有权。

在typosquatting攻击中，攻击者会发布一个与流行软件包名称相似的恶意软件包，希望开发人员拼错软件包名称，无意中获取恶意版本。

通过依赖劫持，攻击者可以获得公共存储库的控制权，从而上传新的恶意版本。

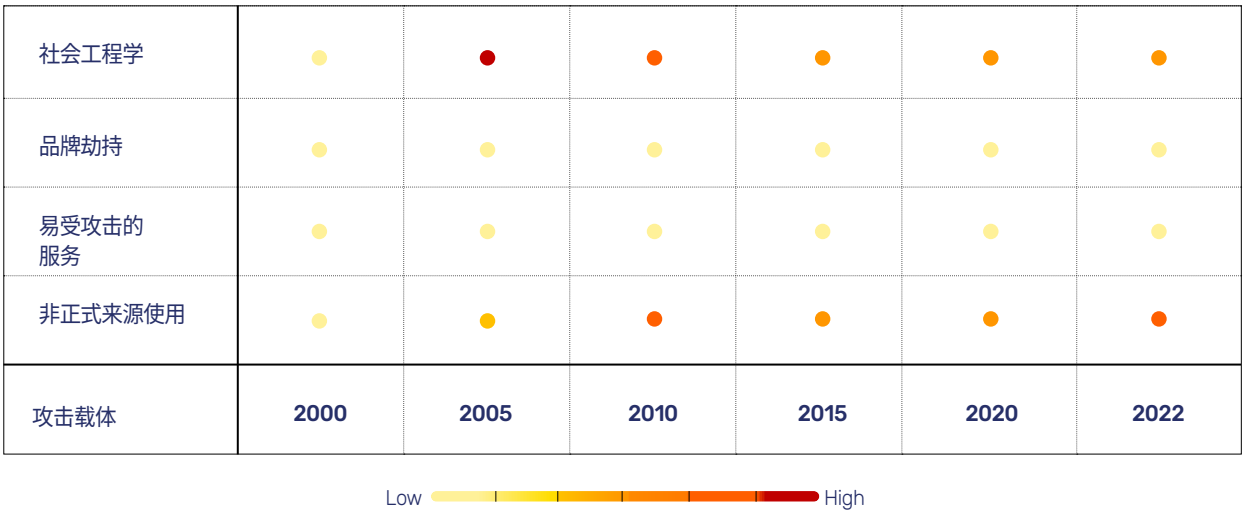
当公共软件源中的恶意软件包与内部软件包名称相同时，就会发生依赖混淆。攻击者就会利用这一特性，诱骗依赖管理工具下载公共恶意软件包，而不是私有的非恶意软件包。
品牌劫持和 typosquatting 是最初的恶意软件包攻击，它们仍然是当今使用的 攻击载体的组成部分。依赖劫持和依赖混淆是最近才出现的。

恶意软件包攻击载体趋势



恶意软件中还有四种常见的攻击载体：非正式来源使用、易受攻击的服务、品牌劫持和社会工程。最常用的攻击载体是非正式来源使用，指的是下载或使用明显不为人所知也没有足够声誉来支持其合法性的网站、公司或产品

恶意软件攻击载体趋势



两者有相似的地方：

- 依赖混淆可被视为与软件包注册表管理器相关的漏洞，这意味着它被视为易受攻击服务的攻击载体。未来，我们将看到依赖管理工具和软件包注册表受到更多脆弱服务的伤害。虽然这是一个复杂的攻击载体，但其中蕴藏着巨大的潜力。

- **品牌劫持**在这两个列表中都有出现，但与一般恶意软件相比，品牌劫持更常用于恶意软件包。这是因为在软件包注册表和开放源代码中存在着明显的攻击潜力，在这些地方，许多人都可以拥有或参与同一个项目，而授权验证却少之又少。由于依赖劫持与品牌劫持非常相似，我们也可以将其纳入这一领域。

- Typosquatting可被视为非正规来源使用，因为对于typosquatting，检查软件包的所有者几乎总能发现它不是一个有信誉的来源。Typosquatting还与社交工程攻击载体有相似之处。它的攻击目标是那些错误输入了自己实际想要的软件包名称的用户。

预测： 虽然它们的名称并不相同，但我们看到通用恶意软件中的每一种攻击载体都有被用于恶意软件包的迹象。由于恶意软件包攻击仍是相对较新的攻击手段，因此社交工程和易受攻击服务的使用都有可能增加。我们预计，使用这两种载体的攻击将会增加，包括恶意软件和软件包注册表本身。

恶意技术

使用恶意软件包的攻击者仍然依赖四种常见技术：安装前和安装后脚本、基本规避技术、shell 命令和基本网络通信技术。虽然数量增加了，但复杂程度却没有增加，尽管我们开始看到不良行为者在基本规避技术之上又增加了中级规避技术。通过快速比较可以看出，恶意软件包所使用的技术有很大的成熟潜力：

相比之下，恶意软件使用成熟和复杂的技术来躲避防御系统，成功潜入并留在受感染的机器上，并在受感染的机器上实现外向网络流量和代码执行。此外，攻击者还利用在其他商业或开源产品中发现的漏洞，以获得更高的成功率或更广泛的能力。

规避技术。尽管恶意软件包中存在这些技术，但它们都是极其基本的技术，如使用 base64 编码或十六进制编码。我们开始看到更多的代码混淆，甚至是时间延迟，试图让动态分析更难检测到恶意活动，但这仍属于基本或中级规避技术。与此同时，通用恶意软件攻击者可以从一长串高级规避技术中进行选择，如反虚拟机、反逆向工程、文件系统和注册表查询等。

持久性。尽管恶意软件包的攻击者可能会持续不断地创建越来越多的恶意软件包，但只有少数攻击者会在受感染的机器上使用持久性技术。与此同时，通用恶意软件攻击者可以利用极其复杂的技术在受感染的机器上持续运行，例如计划任务、快捷方式修改、浏览器扩展、启动密钥等等。

漏洞利用。我们还没有看到恶意软件包达到这种程度。另一方面，一般的恶意软件甚至在感染机器后还会利用漏洞来增强自己的能力。

我们要分析的最后一种恶意技术是指攻击者感染机器后用于部署、执行和通信的方法。恶意软件包使用基本方法在机器上部署、执行和通信，这意味着即使软件包被成功下载到机器上，在部署过程中也相对容易被检测到。另一方面，我们不断看到攻击者使用高级技术来攻击通用恶意软件。

预测：坏人有很多机会重新使用恶意软件包。我们希望能尽快看到更先进的规避技术。恶意软件包将开始使用持久性技术。漏洞利用可能会滞后，因为它不仅难以开发，而且一般只有在特殊情况下才有用--例如，在一个广泛使用的产品中出现了一个新的易于使用的漏洞。最后，我们预计在部署、执行和通信的一般方法中，将迅速出现更多样、更先进的方法。

目标

勒索软件和广告软件目前被认为是最常见的恶意软件类型或一般恶意软件的恶意目标。然而，它们在恶意包中几乎完全不存在。

在依赖性管理工具或软件包注册表中实施这类恶意软件可能有些困难，但这并不是绝对的限制。攻击者开始了解创建和部署这类恶意软件包的潜力。在正在进行的安全猫鼠游戏中，我们知道恶意行为者总是有动力克服他们可能遇到的障碍。

当谈到与加密货币相关的恶意包时，我们会看到带有加密货币的恶意包。一些人尝试过窃取加密货币，尽管与通用恶意软件相比，恶意加密货币攻击的数量远没有达到同类恶意软件的水平。我们将看到针对恶意包中的加密劫持和加密人的恶意包数量增加。虽然机器人有潜力并且仍然存在于通用恶意软件中，但我们看到数量非常有限的恶意行为者为此目的创建恶意软件包。

最后，让我们一起讨论窃取私人信息和侦察，因为恶意包方面存在相当大的重叠。这里，我们再次遇到了一个误导性的边缘案例。乍一看，恶意软件包正在超过通用恶意软件，但这是衡量方法的常见程度而不是其复杂性的衡量标准。使用恶意软件包的不良行为者最常见的目标是窃取私人信息和侦察，而通用恶意软件的行为者已经超越了这些目标。考虑到这一点，我们可能会看到侦察的受欢迎程度下降，因为侦察的动机远低于其他目标。

结论

长期以来，我们一直认为，准备、规划和始终如一地坚持应用安全最佳实践将帮助企业构建坚实的网络安全基础。但是，随着威胁活动的数量和创新性不断增加，企业要想生存下去，就必须超越目前的现状。应用程序是全球经济的命脉，威胁行为者深知这一点。Log4j 和 Solarwinds 漏洞等攻击事件占据了新闻头条，但它们只是每天针对应用程序发起的无情攻击中的一小部分。

幸运的是，我们看到全球公共部门对网络安全的承诺正在增加。包括美国、英国和中国在内的许多国家政府都在增加法规和标准，以提高整个软件供应链的安全性。然而，这只是第一步。由于大多数国家的安全债务不断增加，因此必须找到一种方法，优先处理风险最高的漏洞。我们需要一种新的方法。企业要想明智地管理其安全债务，就需要利用优先级排序和修复工具，针对对其系统和业务影响最大的漏洞进行修复。

关于Mend

Mend （原 WhiteSource），它能轻松地保护开发人员创建的应用程序。Mend 独特地消除了应用程序安全的负担，使开发团队能够更快地交付高质量、安全的代码。凭借成功满足复杂和大规模应用安全需求的良好记录，世界上要求最严格的软件开发人员都信赖 Mend。该公司拥有 1000 多家客户，其中包括 25% 的财富 100 强企业，并管理着开源自动依赖更新项目 Renovate。

更多详细信息，请访问https://www.itbigtec.com/mend

itbigtec 艾体宝

艾体宝科技有限公司

www.itbigtec.com
sales_it@itbigtec.com

广州市黄埔区开泰大道30号佳都PCI科技园6号楼

T> (+86)400-999-3848

各分部：广州 | 成都 | 上海 | 苏州 | 西安 |
北京 | 台湾 | 香港 | 日本 | 韩国

版本：V1.0 - 24/10/15

网络安全与监控方向
(T: 135 3349 1614)

网络安全交流2群

获取更多资料

itbigtec.com