勒索软件防御五步指南

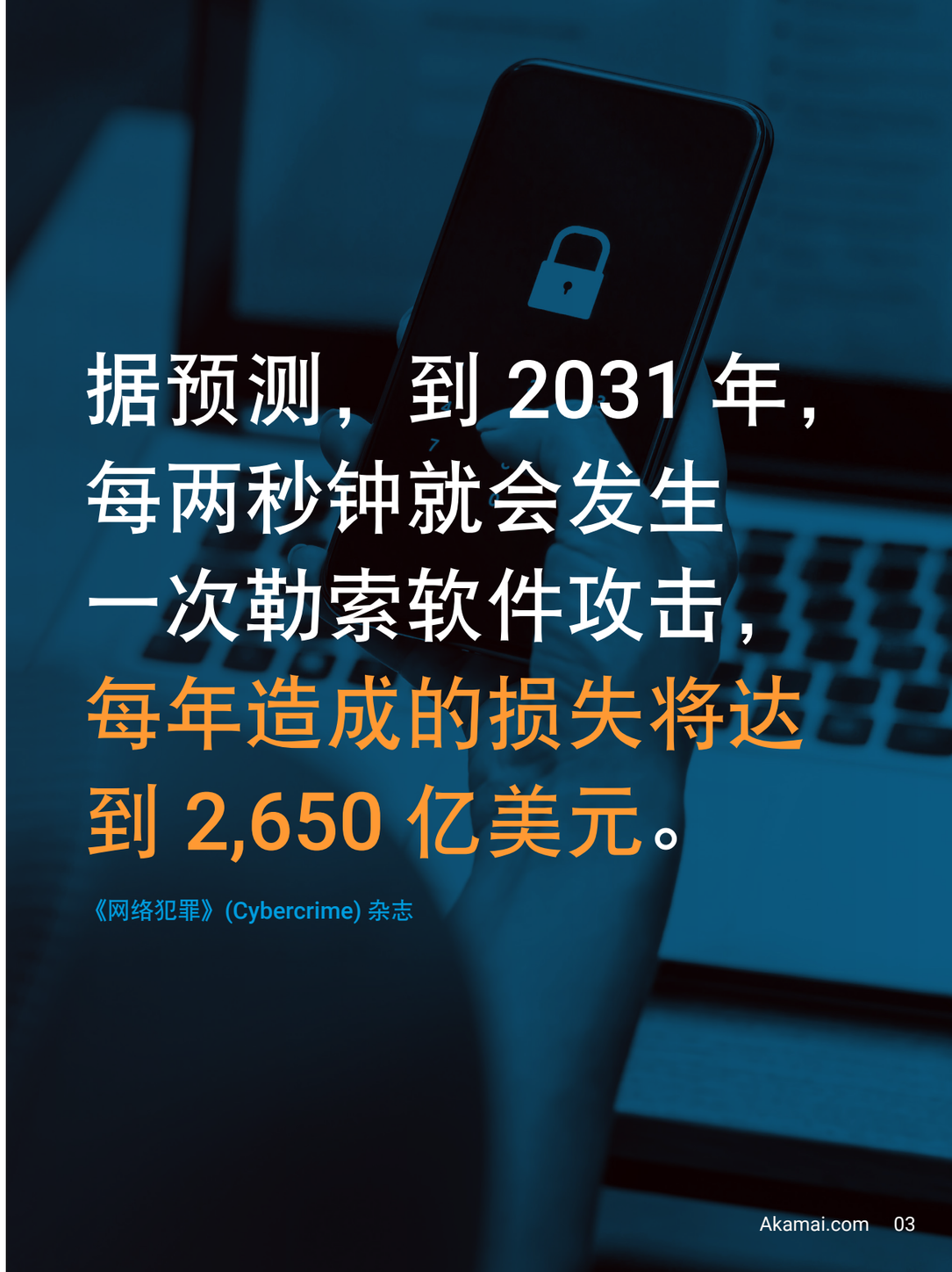
如何强化防御而不再局限于外围防御

目录

简介

勒索软件的兴起和传播

勒索软件一度只是令人烦恼，因为攻击者会用它来加密文件和数据，造成这些内容无法正常访问，但时至今日，它已演变成一种能造成重大破坏的攻击方法。数据永久损失的威胁本身就足以令人不安，更何况网络犯罪分子和民族国家支持的黑客的技术已经足够娴熟，能够利用勒索软件渗透大型企业、国家和地方政府机构、全球基础架构和医疗保健公司等，造成严重破坏。其中许多企业甚至以勒索软件即服务 (RaaS) 的形式提供服务。



勒索软件攻击将让您蒙受损失

2022 年，一次勒索软件攻击导致 7-Eleven 多家门店无法使用收银机或收款，175 家门店被迫暂停营业。同年早些时候，德国的一家石油公司遭受 BlackCat 勒索软件攻击，233 家加油站受影响，Royal Dutch Shell 被迫将货品改运到其他补给站。2021 年 5 月，Colonial Pipeline 攻击造成整个美国东海岸的石油和天然气输送中断。2020 年，Snake 勒索软件攻击造成本田全球业务中断。

如今，陈旧过时的技术、仅关注安全边界和端点的那种所谓“够用就行”的防御策略、培训不足和不良的安全习惯，再加上没有已知的“万能型”解决方案，这些不利因素相互交织，造成各种规模的公司都面临风险。当今的网络犯罪分子已经把勒索软件变成了一种谋生之道，用广撒网的方式加密公司网络中尽可能多的节点，并勒索赎金——从几千美元到数百万美元不等。

但勒索软件危及的并非只有您的利润。勒索软件攻击可带来如下不利影响：停机可能造成业务运营中断、生产力中断和数据被入侵。

一旦公司专有数据遭泄露或被入侵，不仅可能会损害您的品牌形象，而且可能会使您失去客户忠诚度。根据 2020 年的一项调查，80% 的数据泄露涉及客户的个人身份信息 (PII)；32% 的数据泄露涉及知识产权，24% 的数据泄露涉及匿名客户数据被入侵。更不用说，攻击者可能使用这些敏感数据来攻击您的业务，或者进行其他有害的行为，包括销售机密数据。

对于可在网络上快速传播的勒索软件这种威胁，仅仅保护网络边界是远远不够的。

Akamai

阻止横向移动。阻止勒索软件传播。

勒索软件攻击最初始于入侵，其手段通常是钓鱼邮件、网络安全边界中的漏洞或暴力破解攻击，目的是找到突破口并使防御偏离攻击者的真实意图。

一旦攻击侵入某个设备或应用程序，就会跨网络和多个端点继续进行横向移动，从而最大限度地增加被感染的加密点数量。攻击者通常会获得域控制器的控制权，接着盗取凭据，然后找到并加密数据备份，以防止操作人员恢复被冻结的服务。

横向移动是攻击成功的关键。如果恶意软件无法传播到着陆点之外，也就毫无用处。所以，关键在于阻止横向移动。

您的勒索软件威胁抵御策略有多全面?

降低风险

制定绝对可靠的防御策略

检测并防止您网络中的横向移动可以归结为两个主要的重点方面：首先**减少初始攻击媒介**，然后**限制传播路径**。

您可以执行如下操作：限制向互联网公开的服务器数量；通过补丁管理，打上最新补丁，以确保缩小攻击面；设置安全围栏，以减少应用程序间的传播路径；备份数据，以便在发生攻击时快速恢复网络连接，并避免大规模数据丢失。

优先进行安全规划的四种方式

应该将安全纳入企业更广泛的备灾战略、规划和预算当中。也就是说，要提升首席级和董事会成员的安全意识，使其对潜在风险及需要采取的抵御措施保持警惕。

1. 确保将网络安全纳入负责降低企业整体风险的部门职能当中。确保您企业的领导团队具有安全专业知识。
2. 务必为备用开发和网络分段分配专用的预算和资源。
3. 在灾难或不良事件（例如勒索软件攻击）发生之前创建应急响应计划。有组织、有准备，意味着您可以更迅速、更高效地应对事件。
4. 分析每次集成、设计或开发新的产品或服务时的安全影响。问问您自己：我是否在为攻击者敞开新的大门?

勒索软件检测清单

您的网络中正在发生什么情况?

或许您的企业与其他许多企业一样，都将检测勒索软件视为一大难题。如果是这样，您的网络就非常容易遭到攻击。在没有强大的检测能力的情况下，一旦您收到勒索函，则为时已晚：您网络中的大多数节点将被同时加密。

就检测而言，您必须在勒索软件传播时捕获它。您将需要拥有以下项：

强大的监测能力

如果不了解您网络中正在发生什么情况，您就无法检测勒索软件或其他不受欢迎的网络威胁。

分段策略

一旦定义了所有通信并能够考虑这些通信，就能清晰发现不正常的情况，并向您发出警告。

IDS 系统和恶意软件检测工具

这些工具将使用针对已知漏洞或漏洞利用的预定义规则和签名，或更为通用或自动化的异常检测机制，检测勒索软件操纵者的传播企图。

欺骗工具

设置诱饵、蜜罐或者能够识别未经授权的横向移动的分布式欺骗平台，可以通过高保真事件有效发现正在进行的主动入侵活动。

制定勒索软件防御策略

即使有最优秀的外围防御措施，入侵活动也是不可避免的。因此，您必须准备好防御策略，进而最大限度地减弱攻击效果，并阻止攻击在您网络中的传播。寻找能够提供全面安全解决方案的供应商，以检测数据中心横向流量中的威胁并阻止横向移动。

准备

找到一种解决方案，以便您能够识别在您的 IT 环境中运行的每个应用程序和每项资产。借助这种粒度级别的监测能力，您将能够快速映射关键资产、数据和备份，并识别漏洞和风险。通过全面了解您的网络环境，您将能够在遭到入侵期间进行响应并快速激活规则。

防御

您的解决方案应该使您能够创建用于阻止常见勒索软件传播技术的规则。使用软件定义的分段，您可以针对关键应用程序、备份、文件服务器和数据库创建 Zero Trust 微边界。此外还可以创建分段策略，以此来限制用户、应用程序和设备之间的流量，最终阻止横向移动尝试。

检测

实施解决方案，以便在有人尝试获取分段应用程序和备份的访问权限时获得警报。这些被阻止的访问尝试都可能会发展为横向移动。此外，您还应该结合基于信誉的检测，以在出现已知恶意域和进程时获得警报。通过快速发现已成功入侵边界的攻击，您可以尽可能缩短停留时间，并在攻击者基于着陆点进行横向移动之前发现他们。

修复

在检测到攻击时自动启动威胁控制和隔离措施至关重要。应用隔离规则，以快速断开网络被感染部分的连接，同时通过分段策略阻止访问关键应用程序和系统备份。

恢复

最后，您还需要支持分阶段恢复策略的可视化功能。应用分段恢复策略时，将随着网络的各个部分经过验证并“解除警报”，逐渐恢复网络连接。

结论

您对自己现有的防御策略有信心吗?

勒索软件不会消失。事实上，在 2021 年，受到勒索软件影响的企业比例达到 66%，比 2020 年增加了 78%，而且这一比例并无下降的迹象。也就是说，全球将继续遭受更为频繁的攻击，这些攻击将针对体量更大、价值更高的目标，并且攻击者将索要更高昂的赎金——所有这些都会给您的业务带来可怕的后果。现在，您比以往更需要预先规划和风险缓解策略，而不仅仅是基于防御层的方法。

阻断勒索软件在您网络内的横向移动。
让 Akamai 为您展示具体方法。

请访问 akamai.com/guardicore
以了解更多信息。

Akamai 可在您创建的一切内容和体验中融入安全性——无论您在何处进行构建，将其分发到何处，从而保护您的客户体验、员工、系统和数据。我们的平台具备监测全球威胁的能力，这让我们得以帮您调整并增强安全状况，从而实现 Zero Trust、阻止勒索软件、保护应用程序和 API 或抵御 DDoS 攻击，让您信心十足地不断创新、发展和转型。如需详细了解 Akamai 的云计算、安全和内容交付解决方案，请访问 akamai.com 和 akamai.com/blog，或者扫描下方二维码，关注我们的微信公众号。
发布时间：2023 年 5 月

扫码关注，获取最新CDN前沿资讯