SOPHOS

远程勒索软件

恶意远程加密是一种在约 60% 的人为操作的勒索软件攻击中广泛采用的勒索软件技术[1]。大多数领先的端点安全解决方案往往难以应对这种攻击，如果您并非使用 Sophos Endpoint，那么很可能会曝露在这风险中。阅读本指南，了解远程勒索软件的风险以及 Sophos 行业领先的勒索软件防护功能。

什么是远程勒索软件？

远程勒索软件也被称为恶意远程加密，是指利用被入侵的端点来加密同一网络上其他设备上的数据。

在人为操作的攻击中，攻击敌手通常会试图直接部署勒索软件到他们想要加密的设备上。如果初始尝试被阻止（例如，由于目标设备上的安全技术），他们很少会放弃，而是另辟蹊径并反复尝试。

一旦攻击者成功入侵设备，他们可以利用组织的域架构来加密连接域的受托管机器上的数据。所有恶意活动 - 包括入侵、有效负载执行和加密 - 都发生在已经受骇的机器上，从而绕过现代安全堆栈。唯一的入侵迹象是文档在其他机器之间的传输。

80% 的远程加密入侵事故都源于网络上未受管理的设备[2]，不过也有一些入侵事故是从保护不足的机器上开始的，这些机器缺乏阻止攻击者进入设备所需的防御措施。

为什么远程勒索软件如此流行？

这种方法受广泛使用的一个关键因素是其可扩展性：单个未受管理或缺乏保护的端点就足以将整个组织的系统暴露给恶意远程加密，即使所有其他设备都在运行下一代端点安全解决方案。

更糟糕的是，攻击敌手并不缺乏用在这类攻击中勒索软件变体的选择。许多知名的勒索软件家族都支持远程恶意加密，其中包括 Akira、BitPaymer、BlackCat、BlackMatter、Conti、Crytox、DarkSide、Dharma、LockBit、MedusaLocker、Phobos、Royal、Ryuk 和 WannaCry。

导致远程勒索软件流行的另一个重要原因是，大多数端点安全产品在这种情况下效果不佳，因为它们主要专注于侦测受保护端点上的恶意勒索软件文件和进程。然而，在远程加密攻击中，这些进程在被入侵的机器上运行，使得端点保护无法侦测恶意活动。

相反，Sophos Endpoint 包含其业界领先的 CryptoGuard 保护驱动的强大防御，来抵御恶意远程加密的威胁。

Sophos CryptoGuard：业界领先的通用勒索软件保护

Sophos Endpoint 包含多层保护，可防御各种勒索软件，其中包括 CryptoGuard，这是我们独特的反勒索软件技术，包含在所有 Sophos Endpoint 订购中。

与其他端点安全解决方案仅寻找恶意文件和进程有所不同，CryptoGuard 通过分析数据文件中的恶意加密迹象来判断，而不管进程运行在何处。这种方法使其在阻止各种形式的勒索软件攻击方面非常有效，包括恶意远程加密。如果侦测到恶意加密，CryptoGuard 会自动阻止该活动，并将文件回滚到未加密状态。

CryptoGuard 在读取和写入文件时会主动检查所有文件的内容，使用数学分析来确定文件是否已被加密。这种通用方法在业界独一无二，使 Sophos Endpoint 能够阻止其他解决方案未能察觉的勒索软件攻击，包括远程攻击和前所未见的勒索软件变体。

CryptoGuard 是 Sophos Endpoint 中独特的功能之一，包含在所有 Sophos Intercept X Advanced, Sophos XDR 和 Sophos MDR 订购中。此外，该功能默认自动启用，确保组织立即获得对本地和远程勒索软件攻击的全面保护，无需进行微调或配置。

- **通过分析文件内容侦测恶意加密**

  与其他从反恶意软件的角度查看勒索软件的解决方案不同，该方案主要通过侦测恶意代码，CryptoGuard 通过使用数学算法分析内容来查找大规模快速加密的文件，从而侦测恶意加密。

- **阻止本地和远程勒索软件攻击**

  由于 CryptoGuard 专注于文件内容，因此即使在受害者设备上没有运行恶意进程，它也能够侦测到勒索软件加密尝试。

- **自动回滚恶意加密**

  CryptoGuard 创建被修改文件的临时备份，并在侦测到大规模加密时自动回滚更改。Sophos 使用专有方法，不同于其他使用 Windows Volume Shadow Copy的解决方案，而众所周知攻击敌手可以规避这种方法。恢复的文件大小和类型没有限制，最大程度地减少对业务生产力的影响。

- **自动屏蔽远程设备**

  在远程勒索软件攻击中，CryptoGuard 会自动封锁试图在受害者设备上加密文件的远程设备的 IP 地址。

- **保护主引导记录 (MBR)**

  CryptoGuard 还可以保护设备免受加密主引导记录（防止启动）的勒索软件的攻击，以及擦除硬盘的攻击。

发现未受保护的设备

一个单独的未受保护的端点可能使您的组织容易受到远程加密攻击。部署 Sophos Endpoint 可以提供强大的通用勒索软件保护，防止恶意加密，但是首先您如何识别网络上是否有未受保护的设备呢？

这就是 Sophos Network Detection and Respons 网络侦测与响应(NDR)可以提供帮助的地方。Sophos NDR 监控网络流量中的可疑流量，并在此过程中识别环境中未受保护的设备和恶意资产。

为了获得针对远程勒索软件攻击的最强保护，请在环境中的所有机器上安装 Sophos Endpoint，并部署 Sophos NDR 来发现网络上未受保护的设备。

立即提高您对远程勒索软件的保护

恶意远程加密是一种流行的勒索软件技术，但大多数领先的端点安全解决方案都难以阻止。如果您并非使用 Sophos Endpoint，您很有可能处于暴露的状态。

要了解有关 Sophos Endpoint 的更多信息，以及它如何帮助您的组织更好地防御当今的高级攻击，包括远程勒索软件，请立即与 Sophos 顾问或您的 Sophos 合作伙伴联系。您也可以在自己的环境中无购买义务免费试用 30 天。

1 Microsoft Digital Defense Report. https://www.microsoft.com/zh-cn/security/security-insider/microsoft-digital-defense-report-2023

2 Burt, T. (2023, October 5).间谍活动助长了全球网络攻击。Microsoft。https://blogs.microsoft.com/on-the-issues/2023/10/05/microsoft-digital-defense-report-2023-global-cyberattacks/

Sophos 为所有规模的企业提供行业领先的网络安全解决方案，实时保护其防御高级威胁，如恶意软件、勒索软件和网络钓鱼。凭借备受验证的下一代功能，我们可通过由人工智能和机器学习驱动的产品有效地保护您的业务数据。

2023-12-06 (WP-DD)