SOPHOS
Cybersecurity delivered.

阻止勒索软件的端点防护最佳做法

配置您的端点解决方案以提供最佳保护的实用指南

Sophos 白皮书。2022 年 9 月

去年，勒索软件攻击数量增加，造成广泛影响。

在我们的 2022 年勒索软件现状调查中，66% 的受访者称其组织去年受到勒索软件攻击 — 比前一年增加 78%。在近三分之二的事件中 (65%)，攻击者加密数据。

整体来说，修复勒索软件攻击的平均成本为140 万美元，这对业务造成了严重的影响。。此外，90% 的受害者表示，勒索软件攻击影响其运营能力，86% 的私企表示导致其业务/营收上的损失。[1]

勒索软件事件的增长是更广泛网络威胁趋势的一部分：72% 的受访者在去年遇到的网络攻击数量/复杂程度/影响增加。

正确配置的端点防护解决方案是防范勒索软件的最有效方法之一。本白皮书研究勒索软件如何运作，如何阻止，以及配置端点解决方案实现最强防护的最佳做法。

勒索软件攻击如何部署

勒索软件从业者有很多，勒索软件攻击也有很多种。有的具高度针对性，有的采取机会主义。通常攻击者扫描网络，寻找将允许他们进入的漏洞 — 考虑下面攻击加拿大教育机构的勒索软件团伙的说法：

> “你的 Horizon 上有一个旧的重大 Log4j 漏洞并没有修补，所以我们才有办法进入网络。这是一个大范围扫描；并不是我们有意针对您。”

这一说法还凸显攻击者惯常对未打补丁漏洞的利用，这是 Sophos 去年访谈的事件受访者遇到的网络攻击（注意，不完全是勒索软件）中所用的最多的方法。

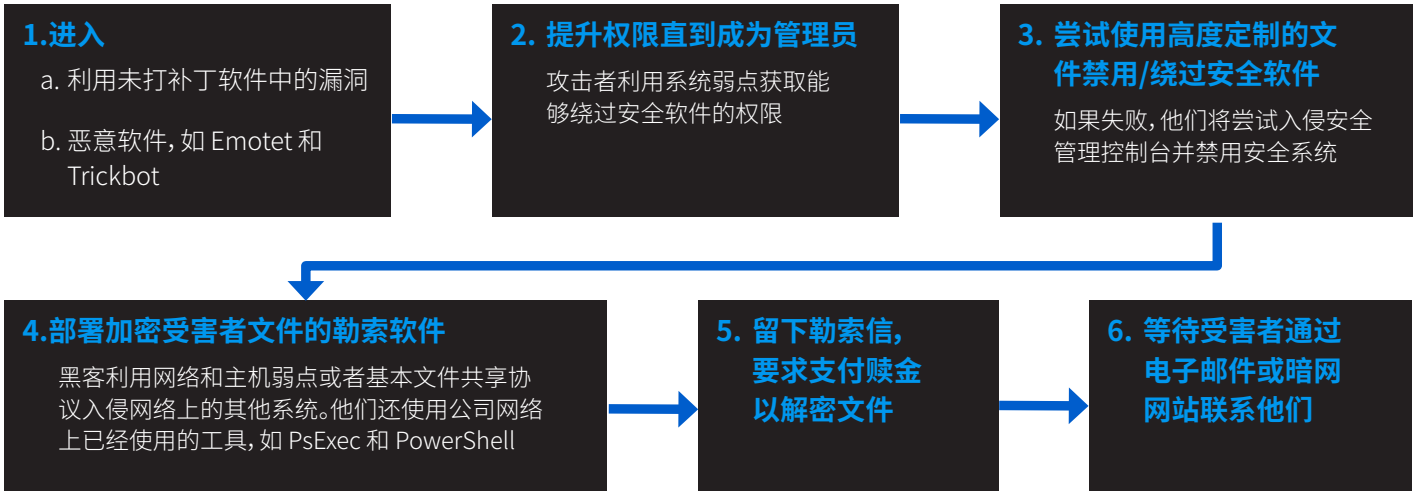
勒索软件攻击数量最近的增加很大程度上可以归结于勒索软件即服务 (RaaS) 模型的增长。现在的趋势是从制作并使用勒索软件的威胁从业者转向利用此模型攻击企业的转变。

借助 RaaS，网络犯罪团体打造勒索软件，出租给其他攻击者。这种方法降低进入门槛，让比以前更多的攻击者能够获取到勒索软件。

攻击者进入受害者环境后，经常用数天、数周或数月时间研究网络，提升权限，外泄数据，安装恶意软件。2021 年，勒索软件攻击的平均驻留时间为 11 天。[2] 这给防御者留下了在攻击前发现并阻止入侵者的时机。

1 2022 勒索软件现状 - Sophos
2 主动攻击对手指南 2022 - Sophos

典型的针对性勒索软件攻击可能如下所示：



远程桌面协议还是勒索软件部署协议？

远程桌面协议 (RDP) 在 2021 年 Sophos 事件响应团队调查的网络事件的至少 83% 中发挥作用，高于前年的 73%。[3]

RDP 和桌面共享工具（如 Virtual Network Computing (VNC)）本身是合法而非常有用的功能，允许管理员远程访问和管理系统。遗憾的是，如果没有正确防护，勒索软件从业者通常利用此类工具。

有趣的是，攻击者使用 RDP 的方式在不断变化。在 Sophos 调查事件的 70% 中，RDP 仅用于内部访问和横向移动。同时，RDP 仅 在 1% 案例中用于外部访问，12% 的攻击显示攻击者将 RDP 用于外部访问和内部移动。

务必阻止攻击者将 RDP 用于外部访问、内部访问和横向移动。

3 主动攻击对手指南 2022 - Sophos
4 主动攻击对手指南 2022 - Sophos

防范勒索软件的最佳做法

保持防范勒索软件需要的不仅仅是具有最新安全解决方案。良好的 IT 安全做法，包括定期员工培训，至关重要。确保您遵循以下 9 个最佳做法：

1.早打补丁，勤打补丁

利用未打补丁的漏洞是 Sophos 调查的 2021 年几乎一半 (47%) 网络事件的根本原因。恶意软件通常依赖主流应用程序的安全缺陷。越早为端点、服务器、移动设备和应用程序打补丁，网络罪犯可以利用的漏洞越少。

2.定期备份，在线和离线保留最近备份副本

在我们的 2022 勒索软件现状调查中，数据被加密的 IT 经理中有 73% 能够通过备份恢复。加密您的备份数据，保持离线和在非现场保存，这样无需担心云备份或存储设备落入坏人之手。此外，定期从备份恢复数据。

3.启用文件扩展名

默认 Windows 设置是隐藏文件扩展名，意味着您必须依赖文件缩略图来识别。启用扩展名，更加方便发现 JavaScript (JS) 文件以及通常不会发送给您和您的用户的其他文件类型。

4.在记事本中打开 JS 文件

在记事本中打开 JS 文件，可阻止其运行任何恶意脚本，并让您检查文件内容。

5.在通过电子邮件接收的文档附件中禁用宏指令

多年前，作为一项安全措施，Microsoft 有意关闭了宏指令自动执行功能。很多感染需要诱导您开启宏指令，不要这样做！

6.小心不请自来的附件

网络罪犯经常利用一个古老的悖论：明知在确定其合法前不应该打开文件，但是如果不打开又不知道文件是不是恶意的。如果有疑问，不要碰。

7.监测管理员权限

定期检查本地和域管理员权限。了解哪些人具有这些权限，删除不需要这些权限的人。以管理员身份登录不要超过必要时间长度。当您用管理员权限时，避免浏览、打开文档，或者执行其他常规工作。

8.规定内部和外部网络访问

不要让网络端口暴露。锁定企业的 RDP 访问和其他远程管理协议。此外，利用双因素身份验证，确保远程用户对 VPN 进行身份验证。

9.使用强密码

听起来很简单，但实际不是如此。可以预测的弱密码可能让黑客在数秒内进入您的整个网络。我们建议设置独特密码，长度至少 12 个字符，使用大小写字母混合，加入随机标点，如 Ju5t.LiKETh1s!

端点安全解决方案的最佳做法

除了网络安全解决方案，使用包含高级防御技术和威胁追踪功能的端点安全或扩展式侦测与响应 (XDR) 解决方案，是防范勒索软件攻击最有效的方法之一。

但是，要使这些技术提供最大网络防护，需要正确配置。

因此我们建议您遵循这七个最佳做法，保护您的端点设备防范勒索软件：

1.采用所有政策，并确保启用所有功能

听起来很明显，但这是从端点解决方案获得最佳方案的十拿九稳方法。政策设计为阻止特定威胁，定期检查已启用所有防护选项可以确保您的端点防范当前和新兴勒索软件。我们建议您：

A) 强化防篡改保护

这防止未经授权修改或移除网络防护软件。恶意软件和攻击者进入系统后的第一个操作是尝试本机禁用或移除任何安全软件。

B) 启用鉴证日志（最好至云端）

如果确实受到威胁，您会想知道发生的情况。但是，这时候大多数数据将不可用，因为攻击者通常擦除系统日志以掩盖其痕迹。或者，您会失去设备访问权。在云端保留活动记录，例如 Sophos Data Lake，确保您可以保留重要信息访问权。

此外，启用侦测无文件攻击技术和勒索软件行为的功能，阻止罪犯渗透您的端点和部署有害勒索软件。

通过 Sophos Central 管理端点防护的 Sophos 客户可以从“Account Health Check”工具获益，该工具自动评估您的帐户配置，发现潜在安全落差，帮助您更改以优化防护。您可以在此处获取该工具。

2.定期检查排除项

排除项阻止扫描值得信任的目录和文件类型的恶意软件。有时候用于减少系统延迟，最小化误报安全提醒的风险。

随着时间推移，不断增加的排除目录和文件类型列表可影响网络中的许多人。能够进入排除目录 — 也许是用户意外移动的 —恶意软件很可能将得逞。

定期检查威胁防护设置内的排除项列表，限制排除项数量。对于任何无法移除的排除项，确保尽可能具体。例如，不要排除数据库的目录或盘符，仅排除带有完整路径的具体文件。这样避免恶意软件绕开您的安全防护，从相同文件夹运行。

3.在安全控制台内启用多重身份验证 (MFA)

MFA 在第一个因素（通常是密码）之后提供额外一层安全。在应用程序中启用 MFA 对于所有可访问安全控制台的用户至关重要。这样做确保端点防护解决方案的访问安全，不容易受到无意或有意更改设置的举动影响，否则可能让您的端点设备容易受到攻击。MFA 对于保护 RDP 也很关键。

4.确保每个端点受到保护并且是最新的

定期检查您的设备，了解是否受保护和最新。无法正确工作的设备不会受到保护，可能容易受勒索软件攻击。端点安全工具通常提供此遥测功能。IT 保健维护计划也有助于定期检查任何潜在 IT 问题。

5.保持良好的 IT 保健

定期评估 IT 保健，确保您的端点和端点上安装的软件以峰值效率运行。这样减轻您的网络安全风险，可以节省修复未来事件的时间。

实施保持 IT 保健的计划，对于防范勒索软件攻击和其他网络安全威胁至关重要。例如：确保 RDP 仅在您需要时运行，定期检查配置问题，监测设备性能，移除不需要的或有害的程序。IT 保健检查可以找出需要更新的软件应用程序（包括安全软件）。确保定期备份数据也是万无一失的方法。

6.主动追踪网络中的主动攻击敌手

在现代威胁环境下，恶意黑客比过去更加狡猾，通常部署合法工具和盗窃的凭据来避开侦测。为了发现和阻止此类“离地”攻击，务必主动追踪高级威胁和主动攻击敌手。发现后，您还需要能够采取合理措施快速阻止。

端点技术，例如端点侦测与响应 (EDR) 和 XDR 提供威胁捕猎和消除。具有此类技术的组织应该充分发挥其作用。

许多组织难以维持全天后覆盖防御高级勒索软件攻击 — 所以托管式侦测与响应 (MDR) 服务是关键。MDR 服务提供由专家交付的 24/7 全天候威胁追踪，他们擅长侦测和响应单纯技术解决方案无法阻止的网络攻击。他们还提供针对人为主导的高级勒索软件攻击的最高防护。

Sophos 能防范勒索软件

我们提供多层威胁防护技术 (Sophos Endpoint Protection)

Sophos Intercept X Endpoint 侦测并阻止 99.98% 攻击运行。采用先进多层防护，包括：

- 防勒索软件行为技术能侦测恶意加密进程，将文件回滚至安全状态。
- 防漏洞利用功能侦测无文件攻击技术
- 人工智能驱动的深度学习引擎能在勒索软件执行之前加以识别并阻止。

内置 Account Health Check 工具自动评估您的帐户配置，发现潜在安全落差，例如未开启的政策或未启用的功能。还提供修复发现的任何问题并优化网络防护的实用指南。

此外，Sophos Central 管理平台自动对访问实施 MFA，增加控制台安全性。

主动威胁捕猎和 IT 保健工具 (Sophos XDR)

Sophos XDR 提供专业级工具，支持您追踪捕猎，保持整个资产内的良好 IT 保健。支持您的团队提出详细问题，发现高级威胁、主动攻击敌手、未保护的设备和潜在 IT 漏洞，并快速阻止它们。

通过访问实时设备数据，长达 90 天磁盘数据，Sophos Data Lake 云存储库中存储的 30 天数据，以及自动生成的可疑项列表，您将获得开始鉴证调查，追踪活跃勒索软件威胁所需的所有信息。

24/7 全天候 MDR 服务 (Sophos MDR)

Sophos MDR 提供 24/7 全天候的精英威胁捕猎团队，代表您侦测和修复攻击。我们的专家累积了数千小时经验，见过并处理过勒索软件攻击者可能向您发动的任何攻击，能带来终极勒索软件防护。

结束语

勒索软件不断进化。虽然我们从未根除勒索软件，但我们的端点防护最佳做法让企业获得最大可能防范最新威胁。

总结：

1. 采用所有政策，并确保启用所有功能。
2. 定期检查您的排除项。
3. 在安全控制台内启用 MFA。
4. 确保所有端点受保护和保持最新。
5. 保持良好的 IT 保健。
6. 搜捕网络中的主动攻击敌手。

在 www.sophos.com/xdr
了解 Sophos XDR

在 www.sophos.com/MDR
了解 Sophos MDR

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。凭借成熟的新一代功能，产品在人工智能和机器学习的支持下，可以有效保护业务数据安全。

© 版权所有 2022。Sophos 有限责任公司 保留所有权利。
注册于英格兰和威尔士（注册号 2096520），注册地址：The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos 是 Sophos Ltd.的注册商标。本文提到的所有其他产品和公司名称是其各自所有者的商标或注册商标。

2020-09-01 ZHCN-WP (DD)

SOPHOS