SOPHOS
Cybersecurity delivered.

保护网络防范勒索软件的最佳做法

提升您对勒索软件和其他网络攻击的防护能力

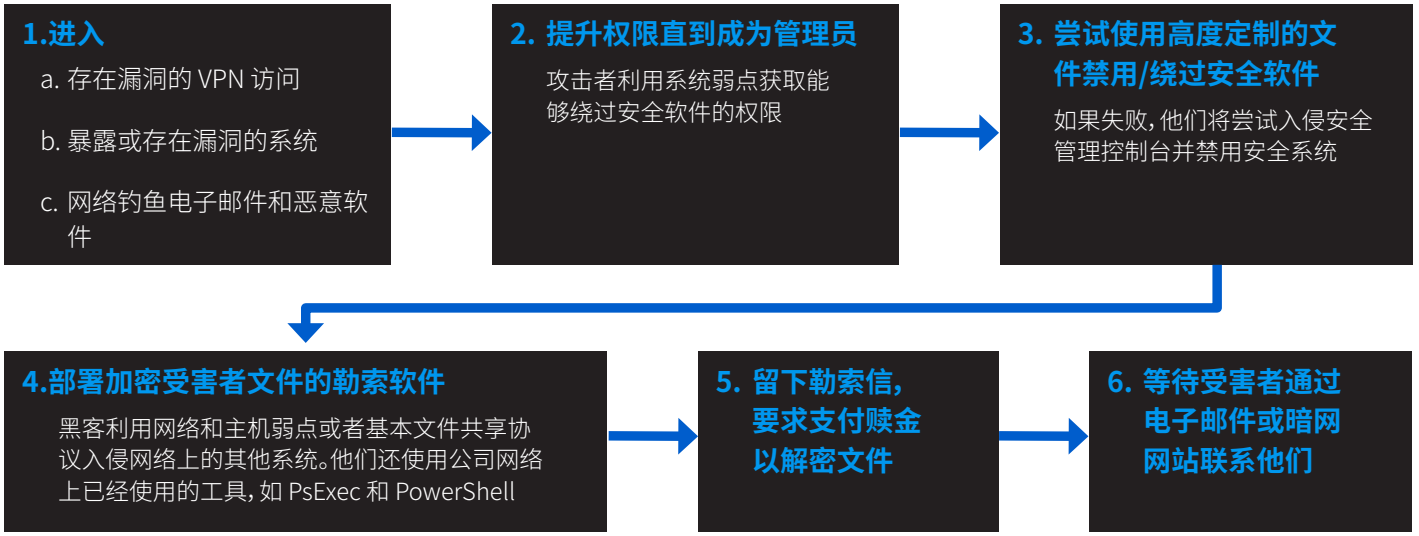
Sophos 白皮书。2022 年 9 月

勒索软件攻击的数量和严重程度不断增加

去年 66% 的企业受到勒索软件攻击，2020 年为 37%。[1] 年同比增长为 78%，证明对手比以往明显更擅长执行大规模攻击。勒索软件的激增很可能也体现了勒索软件即服务模式正在不断取得成功，通过降低部署攻击需要的技能水平，扩大勒索软件可达到的范围。

勒索软件的攻击方式

要了解如何防范勒索软件攻击，首先需要检查其运作方式。典型针对性勒索软件攻击类似这样：



现代勒索软件攻击经常利用合法 IT 和最终用户工具，如 VPN 或远程桌面协议 (RDP) 获取访问权。授权人员在其工作中使用这些工具，使得初始侦测现代勒索软件攻击存在困难。问题的根本原因在于此类工具的使用存在过多暗含信任 — 假定任何可以访问 VPN 或 RDP 的人可以信任，这种做法已经一再证明是不理智的。

1 2022 年勒索软件现状，Sophos - 对 31 个国家 5,600 名 IT 专业人员的独立调查。

如何防御勒索软件攻击

三个网络安全措施可以帮助减轻勒索软件攻击的风险。

1. 消除远程访问的暴露

许多人认为虚拟专有网络 (VPN) 可防范勒索软件攻击。这种认知是错误的，VPN 是恶意黑客很容易使用的攻击工具。当然，随着过去两年数百万员工转为在家上班，最近远程访问 VPN 使用的迅速增加，这种攻击媒介变得更加有吸引力。攻击者意识到此类家庭网络保护程度差并脆弱，是很容易攻破的目标。

2021 年的一个最高调勒索软件攻击祸及一家美国管道公司，导致其在美国东部和南部的大多数客户中断了燃油供给。攻击过程中，网络罪犯利用了远程访问 VPN。

大多数过时的 VPN 客户端还包含可以利用的漏洞，进一步增加保护网络访问抵御外部威胁的挑战难度。这促使执法部门，如 FBI、国土安全局和 CISA（网络安全和基础设施安全局）发布关于基于远程访问 VPN 基础设施的攻击可能性的警告。

最佳做法 — 用 ZTNA 替代远程访问 VPN

零信任网络访问 (ZTNA) 是远程访问 VPN 的现代替代品。它消除了 VPN 提供的固有信任和广泛访问权，采用零信任原则 — 不信任一切，验证一切。相比远程访问 VPN，ZTNA 提供更好的安全性，更方便的管理，更好的可见性，更好的用户体验。

ZTNA 消除存在漏洞的 VPN 客户端，利用多重因素身份验证 (MFA) 和设备运行状态以控制访问权，仅为特定网络应用程序提供访问权，对网络进行有效细分。还应注意，白宫发布了零信任架构命令，所有联邦机构到 2024 年必须遵守。

通过暴露的远程桌面系统 (RDP) 和其他系统杜绝除暴露机会

远程管理工具，如 RDP、虚拟网络计算 (VNC) 和其他远程管理解决方案，允许远程员工访问和管理系统。遗憾的是，如果没有正确的防护，此类工具也为攻击者提供便捷通道启动勒索软件攻击。

不保护RDP和其他远程管理解决方案的安全，会使你受到勒索软件的攻击。网络罪犯经常使用大范围扫描和穷举破解工具，尝试数十万次用户名和密码组合，直到获得正确组合。有时候，他们将利用这些凭据立刻发起攻击。有时候，他们将这些凭据出售给其他攻击者团体。

“Horizon 上有一个旧的关键 Log4j 漏洞没有修复，我们最初能够介入的方法如下。这是一个大范围扫描；并不是我们有意针对您。一旦进入您的 horizon VM，我们转储凭据，获得一些域管理员，破解哈希 [并] 能够纵向移动。”

成功的勒索软件攻击者关于其如何获得访问权的说法

上面的说法来自一个威胁黑客团体，他们通过大范围扫描发现的 VMware Horizon 的未打补丁漏洞，获得某组织的访问权并进行勒索。这凸显了保持系统固件和软件打补丁并保持最更新的重要性。

最佳做法 — 消除直接外部访问

阻止通过防火墙的所有访问，仅通过 ZTNA 启用访问，保护远程系统访问。这有效移除了直接外部访问。

检查所有防火墙规则，确保任何 RDP 或远程管理系统不会通过端口转发或 NAT 规则暴露。此外，确保通过 ZTNA 严格控制安全访问。这证明只有通过 MFA 和运行状况证明其身份的授权用户与设备可以获得访问权。

此外，考虑新的安全身份验证技术，如 Windows Hello for Business。当然，还要保持基础设施打补丁和最新，防止旧漏洞成为容易攻破的目标。

2. 阻止恶意软件和勒索软件通过网络钓鱼和下载进入

另一个古老的攻击方式是诱骗用户回复网络钓鱼电子邮件和/或打开恶意电子邮件。现在，您需要现代防火墙、端点和消息防护与最新机器学习和沙箱技术一起协同工作，发现不断进化的尝试访问您网络的针对性威胁。理想情况下，您需要阻止此类威胁进入您的网络，或者如果已经进入网络，则隔离并防止其移动。

最佳做法 — 采用零日威胁防护

确保您有最新的网络钓鱼和恶意电子邮件讯息防护，禁止此类威胁进入用户收件箱。此外，确保您的防火墙具备深度数据包检查 (DPI) 技术，包括用于检查加密的有效载荷的 TLS 1.3 解密，用于新的零日威胁的机器学习分析，以及在运行时评估传入文件的沙箱。教育您的用户如何识别潜在网络钓鱼威胁。而且确保您的端点具备针对凭据盗窃、漏洞利用攻击和勒索软件的最佳防护。

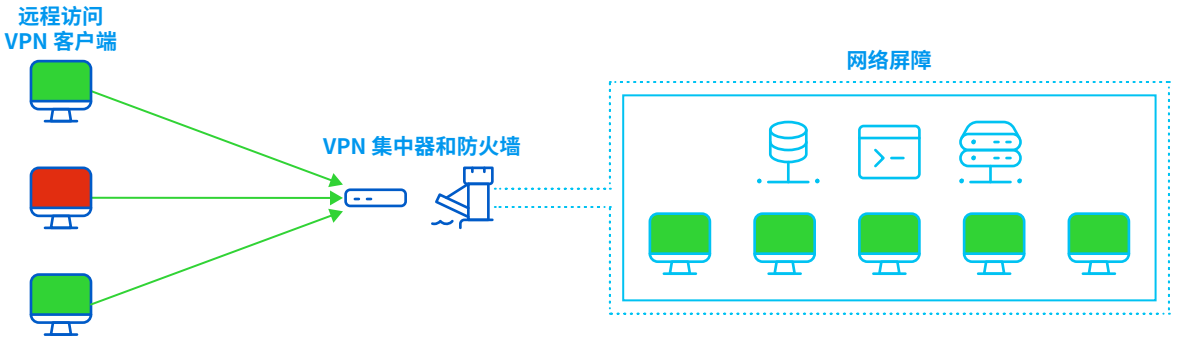
要隔离进入您网络的威胁并阻止其移动，可以采用我们在下一节介绍的一些最佳做法。

限制横向移动

在网络攻击过程中，网络安全解决方案限制其在网络内移动 — 或横向移动的能力至关重要。

遗憾的是，大多数网络就像中世纪的城堡 — 通过俗话所说的的城堡外墙和护城河构成网络资源的安全外围。VPN 相当于授权用户进入安全外围的安全门房。但是，一旦网络罪犯进入网络，可以完全访问其外围内的一切内容。这种网络内的移动自由度也适用于勒索软件等威胁。

网络罪犯将 RDP 和其他管理系统以及未托管设备作为进入点。他们还利用此类进入点在网络内横向移动。



最佳做法 —微划分您的网络

和零信任一样，这对现代网络至关重要。您应运用下面三个最佳做法设计您的网络架构：

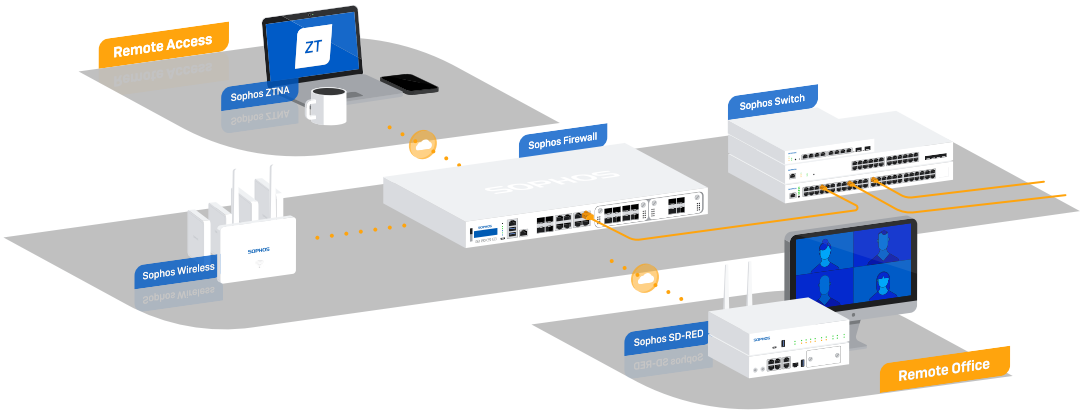
1. **划分您的网络。**创建小区域或 VLAN，通过托管交换机和防火墙连接，在分段之间应用防恶意软件和 IPS 防护。这让您可以识别和阻止威胁尝试在网络上横向移动。
2. **使用 ZTNA。**微划分网络应用程序，仅允许授权用户访问其需要的资源。这样，如果用户设备被攻破，威胁未被侦测到，可以快速消除威胁。Sophos ZTNA 更进一步，在设备被攻破后，完全移除访问权。
3. **利用 Sophos Synchronized Security 等技术。**Synchronized Security 让您可以自动响应网络上的活跃威胁，隔离，并阻止其横向移动。可以立刻发现威胁，通知健康设备忽略被攻破主机的任何流量，而 Sophos Switch 自动切断来自被感染设备的数据包，Sophos Firewall 进一步限制被攻破主机访问网络其他部分。

防范勒索软件的网络安全最佳做法

总的来说，您可以利用以下最佳做法，保护您的网络防范勒索软件和其他网络威胁：

- **微划分网络。**这样您可以限制威胁横向移动。利用 Sophos ZTNA 微划分网络应用程序的访问。最重要的是，利用 Sophos Firewall 和 Sophos Switch 微划分内部网络资源。此外，利用 Sophos SD-RED 划分并安全连接远程设备和位置。
- **用 ZTNA 替代远程访问 VPN。**移除潜在存在漏洞的旧 VPN 客户端，消除常见攻击渠道。升级到现代 ZTNA 解决方案，如 Sophos ZTNA，集成 Sophos 下一代端点防护，可以通过从单一供应商的单一控制台管理的单一代理，妥当保护您的用户设备、身份、应用程序和数据访问、网络。
- **实施最强防护**您应对防火墙、端点、服务器、移动设备和远程访问实施最佳防护。
  - 确保您的防火墙具有 TLS 1.3 检查、下一代 IPS 和串流 DPI，以及机器学习和沙箱以防范最新零日威胁。Sophos Firewall 包含所有此类技术，紧密集成以提供强大防护和性能，这样您可以从防火墙投资获得最佳价值。
  - 而且确保您的端点具备防范凭据盗窃、漏洞利用攻击和勒索软件的现代下一代防护功能。Sophos 一直被评为下一代端点防护解决方案的顶级提供商。我们保护您的端点、移动设备和服务器，和其余 Sophos 产品一样，允许您从同一个云管理控制台管理。
- **减少网络攻击面。**检查您的防火墙规则，消除通过 VPN、NAT 或端口转发的任何远程访问或 RDP 系统访问。此外，确保妥当保护任何流量。Sophos Firewall 通过卓越的可见性、仪表板、报告和规则管理功能轻松实现这一点。
- **保持您的固件和软件打补丁并且保持最更新。**这对于防火墙或远程访问软件或客户端等任何网络基础设施尤其重要，但对所有系统都同样重要，因为每个更新包含以前发现漏洞的重要安全补丁。Sophos 允许您保持所有网络安全产品自动更新。
- **使用 MFA。**确保您的网络在零信任模型上运行，每个用户和设备必须通过验证身份持续取得信任。此外，实施强密码政策，考虑采用身份验证解决方案，如 Windows Hello for Business。所有 Sophos 产品支持您首选身份验证提供商的 MFA。
- **立即响应网络攻击。**利用自动化技术和真人的专业知识，加快网络事件响应与修复。
  - 确保您的网络安全基础设施帮助您自动响应活跃攻击，这样您可以在导致严重破坏前隔离被攻破的主机。只有 Sophos Synchronized Security 能够在您需要时提供您真正需要的响应水平。
  - 部署托管式侦测与响应 (MDR) 服务，例如 Sophos MDR。借助 Sophos MDR，威胁专家团队不断监测和响应事件阻止其变为问题，因此您无需担心。

用 Sophos 保护您的网络



Sophos 提供完全保护网络防范攻击需要的一切，包括防火墙、ZTNA、交换机、无线、远程边缘设备、消息防护、MDR 和下一代端点防护，用于所有设备和服务器。最大的优点是全部从一个云管理控制台 — Sophos Central — 管理，集成在一切以提供 Sophos Synchronized Security 和跨产品威胁侦测与响应或扩展式侦测与响应 (XDR)。

Synchronized Security 确保您的 Sophos 产品不断共享遥测和运行状况数据，这样您可以快速响应网络攻击。侦测到被攻破的主机后，您的健康端点自动忽略流量，交换机切断被攻破主机的数据包，防火墙阻止对网络其余部分的访问，直到解决问题。任何其他网络安全系统都不能比拟 — 我们让网络安全更简单更有效。

Sophos XDR 是行业唯一 XDR 解决方案，同步本机防火墙、端点、服务器、电子邮件、电子邮件、云和 Microsoft 365 安全，提供企业环境的全盘视图。它为专业安全运营中心团队和 IT 管理员提供丰富数据集和深度分析，用于威胁侦测、调查和响应。

如果您发现网络安全过于复杂，过于困难，变化过快，无法自行有效管理，让我们协助您。Sophos MDR 保护全球超过 11,000 家企业，提供全球威胁专家团队带来的 24/7 全天候威胁追踪与消除。

重要的是：Sophos 提供一系列网络安全和服务，帮助您轻松保护网络防范勒索软件。

访问 www.sophos.com
了解 Sophos 如何保护您的网络

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。

2022-09-12 ZHCN-WP (DD)

SOPHOS