2020 SONICWALL 网络威胁报告

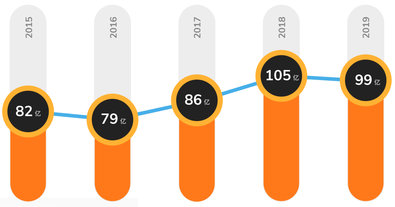
您的数字帝国的疆界是无限的。这个空间曾经是有限和可防御的，现在却变成了无边无际的领域——一个包括设备、应用、装置、服务器、网络、云和用户等印记的广阔海洋。

探索 SonicWall 的独家威胁情报，以帮助您更好地了解网络罪犯的想法，并针对他们的下一步行动做好充分准备。

恶意软件减少，但更具针对性和隐蔽性

99 亿

次恶意软件攻击是 SonicWall 在 2019 年记录的数值*，比 2018 年创纪录的 105.2 亿次下降了 6%。



勒索软件发现了新目标

1.879 亿

网络罪犯使用勒索软件对目标受害者进行外科手术式攻击，这些受害者是更有可能为他们拥有的敏感数据或可支配资金（或两者兼而有之）付款的人。

在 2019 年，这意味着 1,879 亿次勒索软件攻击中有许多是针对州、省和地方政府以及教育系统的。

加密窃取减少

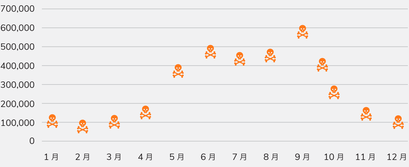
比特币和互补加密货币的价格在基于 Coinhive 的加密劫持恶意软件和合法的 Coinhive 挖矿服务之间造成了难以为继的局面。

78% ↓ 在 Coinhive 倒闭之后，加密劫持攻击次数在 2019 年下半年下降了 78%。

第 3 季度无文件恶意软件攻击达到峰值

无文件恶意软件仅作为基于内存的构件存在，并不将其恶意活动的任何部分写入计算机硬盘，这使它非常不容易被取证策略发现。攻击次数峰值出现在第三季度，仅 2019 年 9 月 SonicWall 记录的攻击就超过 570,000 次。

2019 年无文件恶意软件攻击次数



加密威胁继续稳步上升

精明的网络罪犯继续使用 TLS/SSL 加密来掩盖其攻击，以逃过传统安全控制措施的检查。在 2019 年，SonicWall Capture Labs 威胁研究者们记录，通过 TLS/SSL 连接发送的恶意软件同比增加 27.3%。

27% ↑ 2019 年通过 TLS/SSL 连接发送的恶意软件增加。

IOT 攻击次数上升

2019 年，SonicWall 发现，IoT 恶意软件增加了 5%，总量达到 3,430 万次攻击。

但是，每天都有大量新的 IoT 设备连接，因此不但要预见到 IoT 恶意软件攻击会增加，而且要对此有所规划。

3,430 万 ↑

针对下一步做好准备

访问 SonicWall.com/ThreatReport 以下载完整的 **2020 年 SonicWall 网络威胁报告。**您将获得关键威胁情报，以帮助您更好地了解网络罪犯的想法，并针对他们的下一步行动做好充分准备。

获取报告

SONICWALL

SonicWall.com

*作为最佳做法，SonicWall 经常优化数据收集、分析和报告的方法。其中包括调整数据清理、改变数据源和合并威胁源。先前报告中发布的数据可能已在不同时间段、地区或行业进行了调整。

本文件包含的材料和信息（包括但不限于文本、图形、照片、艺术品、图标、图像、徽标、下载、数据和汇编）属于 SonicWall 或原创作者，受适用法律保护，包括但不限于美国和国际版权法律和法规。

© 2020 SonicWall。保留所有权利。