勒索软件：现状

它真实存在，极为复杂，且变化多端！

丢失敏感的专有数据

经济损失

造成破坏

信誉损害

代价不菲的恶意软件。

识别不断增加的威胁

2015

在 FBI 的“2015 年热点”名单中排名**第 3**[1]

发展势头增强

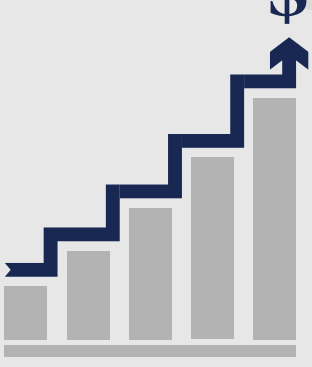
在 FBI 的 2400 多件投诉中敲诈金额为 **2400 万美元**[2]

挫败了金额高达 **6000 万美元** 的 Angler 漏洞攻击包攻击活动[3]

2016

“勒索软件爆发年”

前 3 个月的敲诈金额为 **2.09 亿美元**[4]



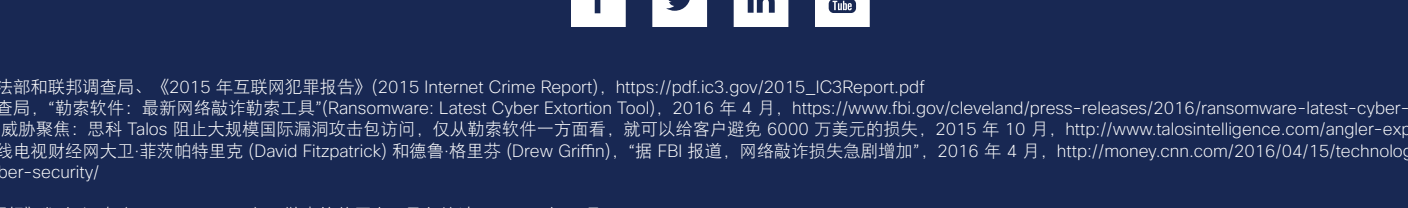
预计 2016 年的非法获利将达到 **10 亿美元**[5]

企业用户目标 **增加了 6 倍**[6]

了解攻击媒介

漏洞攻击包是攻击者用于传播恶意软件的工具。
通常通过以下方式传播：

- **邮件：** 包含恶意链接或附件的网络钓鱼消息和垃圾邮件
- **Web 服务器：** 访问网络的入口
- **基于 Web 的应用：** 通过社交媒体和即时消息传播的加密文件
- **恶意广告：** 由受感染站点下载引发



采用架构性方法 **防止攻击**：

- DNS 层、终端、邮件、Web 和网络层保护
- 保护网络内外的设备安全
- 准备快速检测并遏制恶意软件的移动

检测并摧毁 勒索软件

思科 Talos 每年通过挫败勒索软件攻击，为用户避免 **6000 万美元**损失[7]

Angler 是最大也是最高级的漏洞攻击包之一，用于目标恶意广告活动中

每天有 **90,000 名受害者**中招，
每年造成近 **150 个代理服务器**丧失服务能力，
年损失金额高达 **3000 万美元**

立即了解详情

访问 **cisco.com/go/ransomware**，
了解简单、开放、有效的思科自动化安全方法。

CISCO

[1] 美国司法部和联邦调查局、《2015 年互联网犯罪报告》(2015 Internet Crime Report)，https://pdf.ic3.gov/2015_IC3Report.pdf
[2] 联邦调查局，“勒索软件：最新网络敲诈勒索工具”(Ransomware: Latest Cyber Extortion Tool)，2016 年 4 月，https://www.fbi.gov/cleveland/press-releases/2016/ransomware-latest-cyber-extortion-tool
[3] Talos，威胁聚焦：思科 Talos 阻止大规模国际漏洞攻击包访问，仅从勒索软件一方面看，就可以给客户避免 6000 万美元的损失，2015 年 10 月，http://www.talosintelligence.com/angler-exposed/
[4] 美国有线电视财经网大卫·菲茨帕特里克 (David Fitzpatrick) 和德鲁·格里芬 (Drew Griffin)，“据 FBI 报道，网络敲诈损失急剧增加”，2016 年 4 月，http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/
[5] Ibid。
[6] 《安全周报》凯文·汤森 (Kevin Townsend)，“勒索软件历史记录与统计”，2016 年 6 月，http://www.securityweek.com/history-and-statistics-ransomware
[7] 思科 Talos，威胁聚焦：思科 Talos 阻止大规模国际漏洞攻击包访问，仅从勒索软件一方面看，就可以给客户避免 6000 万美元的损失，2015 年 10 月，http://www.talosintelligence.com/angler-exposed/