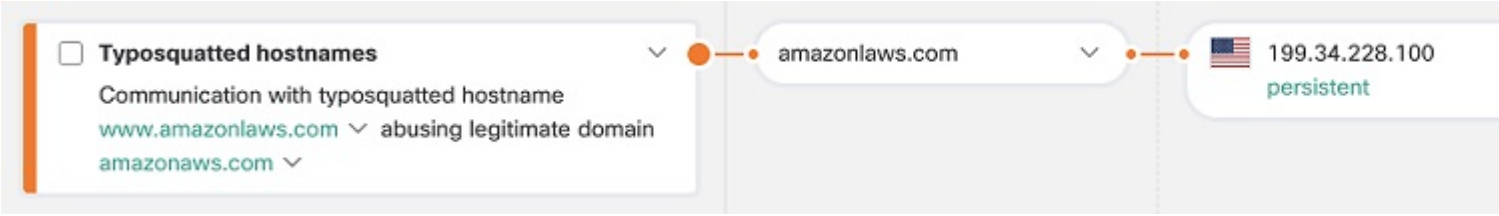
2021 年 3 月

2021 年 3 月发布的思科基于云的机器学习全局威胁警报更新。

新误植域名分类器

误植域名是一种 URL 劫持形式，它依赖于用户在其 Web 浏览器中输入 URL 时出现的印刷错误（打字错误）。这会导致用户被定向到攻击者的替代网站。误植域名 URL 看起来类似于合法 URL，例如：

图 *1:* 示例：添加了其他字母的误植域名主机名



误植域名URL通常导向在线欺诈，例如用于从广告中获利的广告页面或用于窃取用户信息的网络钓鱼页面。

图 *2:* 示例：以有意前往 ***Amazon AWS*** 的用户为目标的广告页面

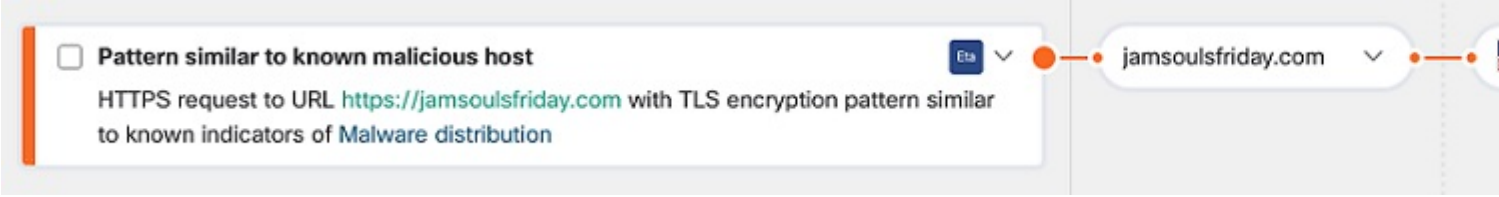
新的分类器旨在保护用户免受针对大多数常用域的误植域名域的攻击。分类器通过计算域的相似性来有效识别与最常用域相似的域。然后，分类器根据其他参数（例如，误植域名域的期限）确定威胁的严重性。

这可以在**警报** > **警报详细信息** > **安全事件**中看到。

新 TLS 模式分类器

新的分类器基于传输层安全 (TLS) 指纹技术构建。考虑到来自加密流量分析 (ETA) 的TLS报头以及其他全局和本地情景功能，分类器根据其TLS足迹检测可疑和恶意应用。通过分析已加密通信，分类器扩展了针对通过 HTTP 通信的威胁的模型的功能。

图 *3:* 示例：类似于已知为恶意的主机的 ***TLS*** 模式



这可以在**警报** > **警报详细信息** > **安全事件**中看到。