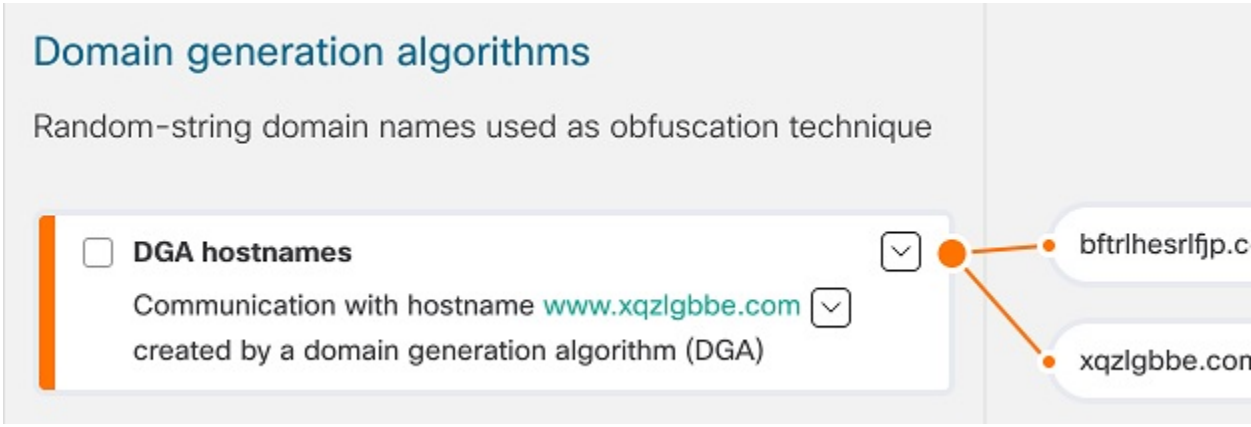
2021 年 4 月

2021 年 4 月发布的思科基于云的机器学习全局威胁警报更新。

新 DGA 2.0 分类器

攻击者使用域生成算法 (DGA) 随机生成主机名，以绕过具有阻止功能的安全产品。这些算法通常用于在僵尸网络和广告软件中进行通信。由于它们是动态生成的，因此可以成功绕过依赖静态、基于签名的监视列表的安全产品，否则这些产品会被阻止。

图 *1:* 示例：*DGA* 为混淆阻止程序生成的随机字符串



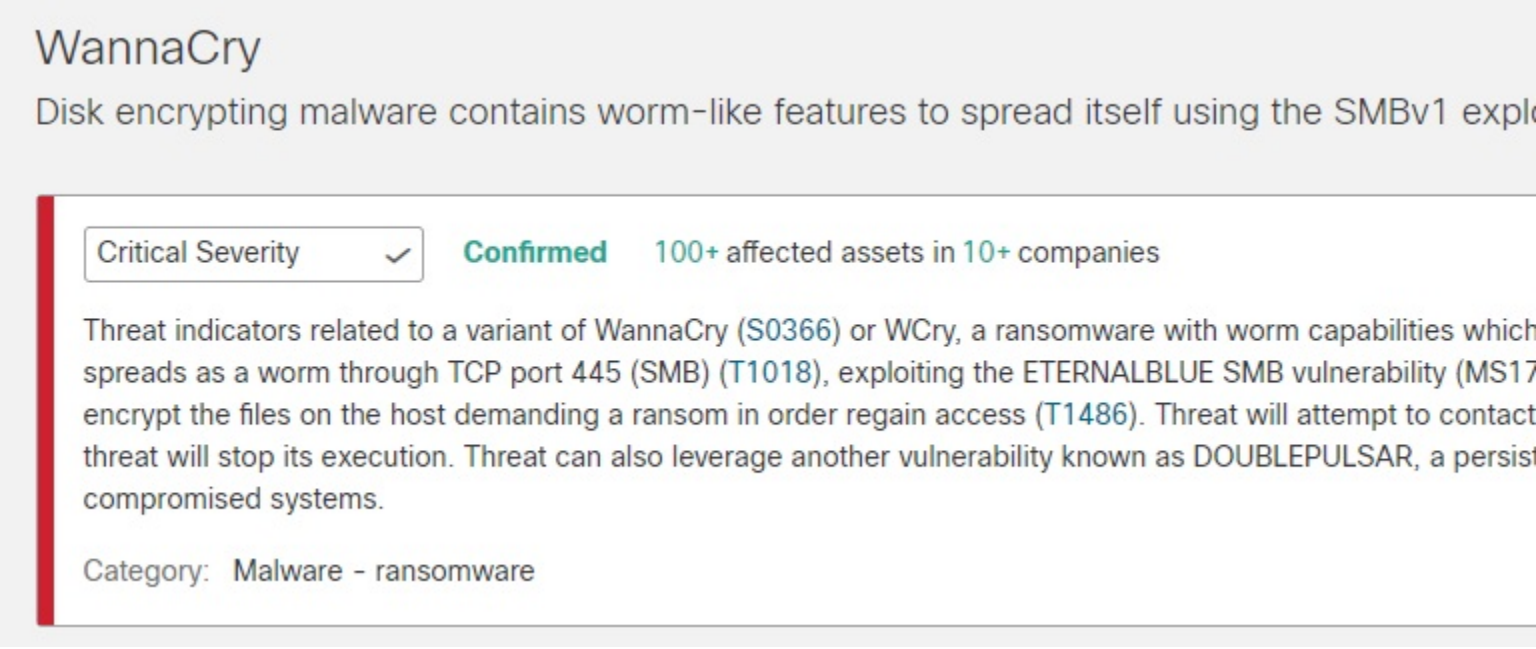
虽然自 2015 年以来，全局威胁警报已支持 DGA 域检测，但 DGA 2.0 分类器是基于神经网络（用于文本处理的最先进解决方案）而不是较旧的随机域林构建的新模型。这种架构更新和新设计的训练集可以使召回率（正确的正误差率数量）翻倍，同时产生更少的错误的正误差率。

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

警报描述中的新 MITRE 参考

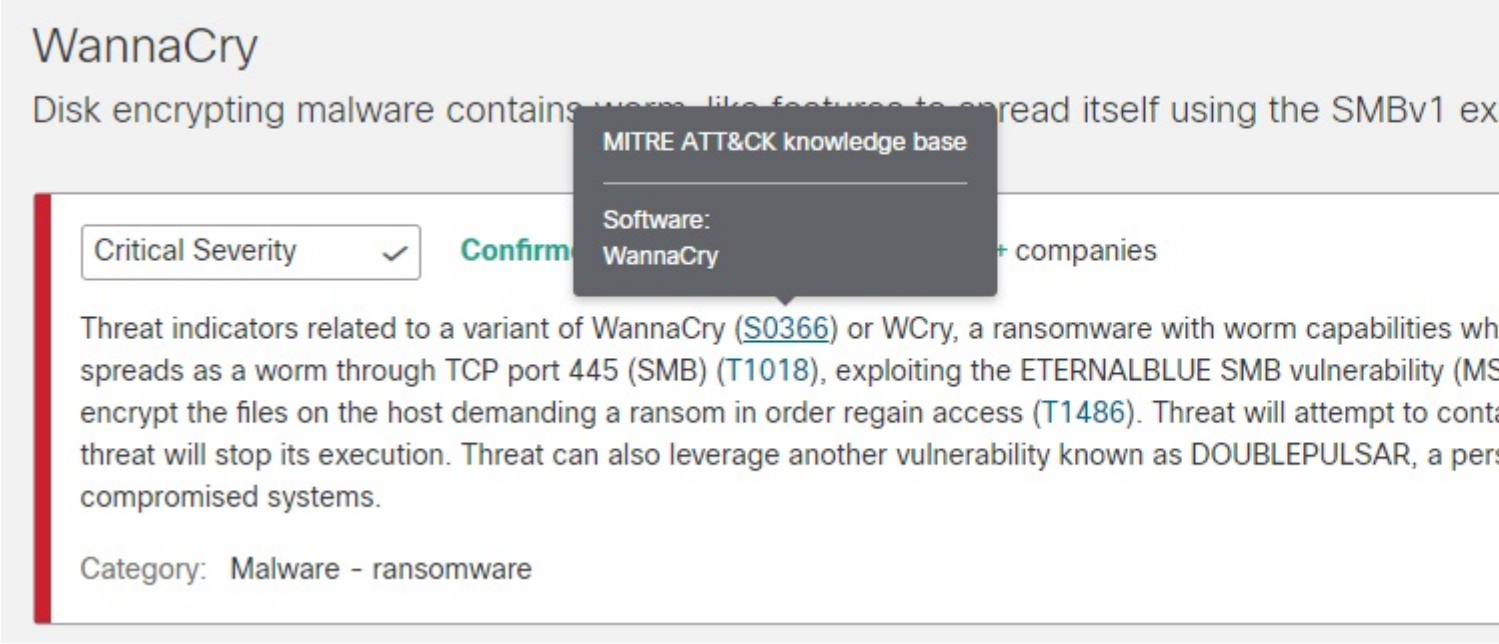
现在，我们已直接在警报的说明中添加 MITRE 引用（如果可用），以便您可以方便地访问补充信息。

图 *2:* 示例：*WannaCry* 说明中的四个 *MITRE* 引用（*S0366*、*T1018*、*T1210*、*T1486*）



正在查找有关警报及其说明的其他详细信息？点击 ID 号码...

图 *3:* 示例：*S0366* 的 *MITRE ATT&CK* 知识库的嵌入式链接



...打开一个新的浏览器页面，将向您显示 MITRE ATT&CK 知识库，其中包含有关特定威胁的更多信息和详情。

图 *4: MITRE ATT&CK* 页面，包含有关 *S0366* 的更多信息和详情