



2021 年 4 月

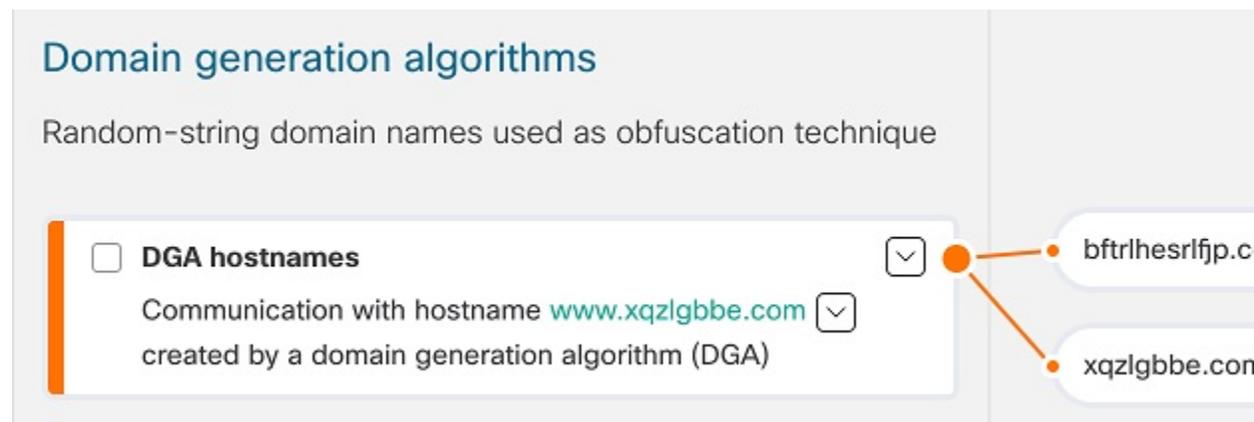
2021 年 4 月发布的思科基于云的机器学习全局威胁警报更新。

- [新 DGA 2.0 分类器，第 1 页](#)
- [警报描述中的新 MITRE 参考，第 2 页](#)

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域



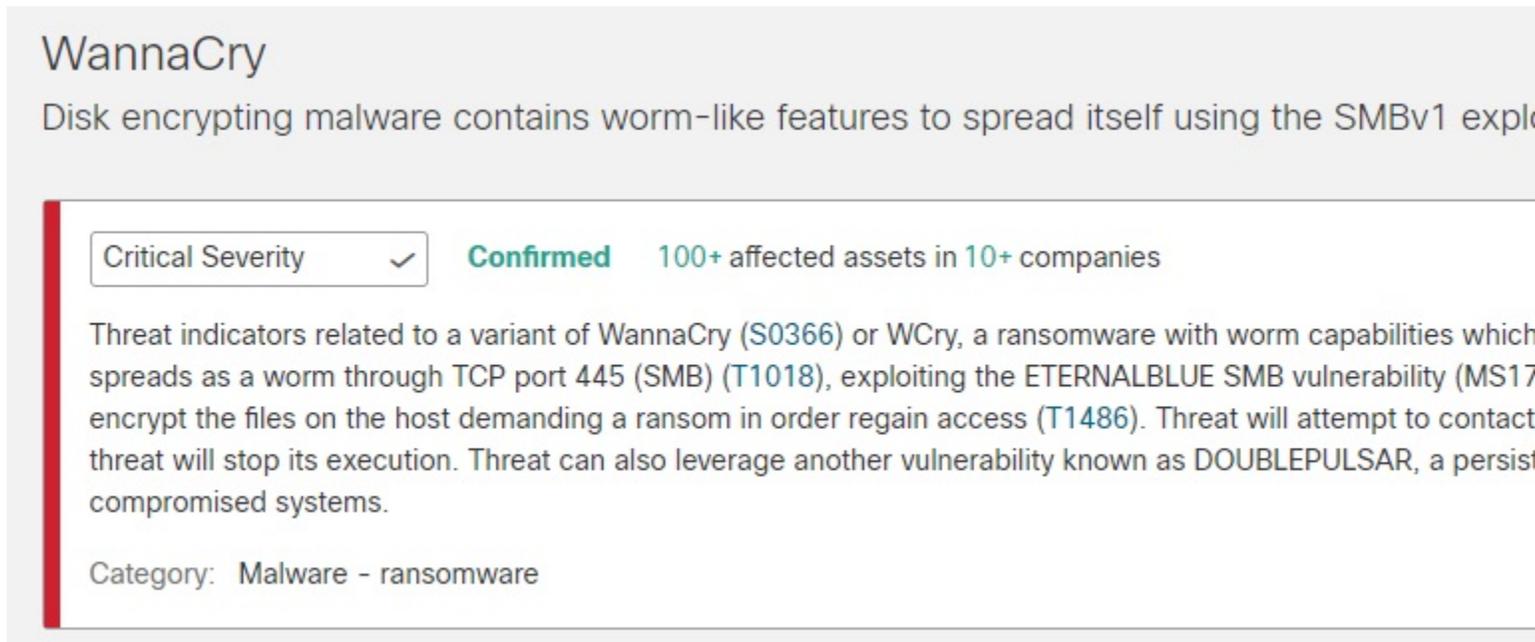
虽然自 2015 年以来，全局威胁警报已支持 DGA 域检测，但 DGA 2.0 分类器是基于神经网络（用于文本处理的最先进解决方案）而不是较旧的随机域林构建的新模型。这种架构更新和新设计的训练集可以使召回率（正确的正误差率数量）翻倍，同时产生更少的错误的正误差率。

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。

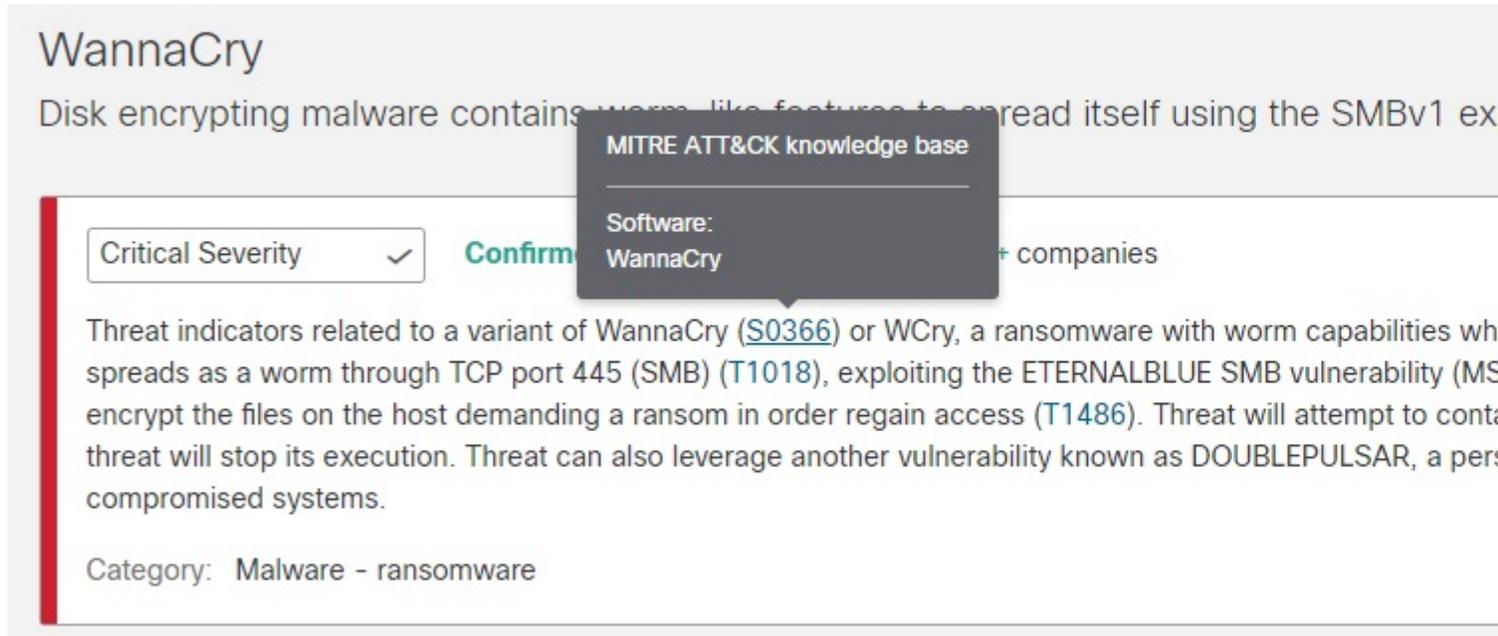
图 2: 示例: *WannaCry* 说明中的四个 MITRE 引用 (S0366、T1018、T1210、T1486)



The screenshot shows a security alert for 'WannaCry'. The title is 'WannaCry' and the subtitle is 'Disk encrypting malware contains worm-like features to spread itself using the SMBv1 exploit'. Below the title, there is a severity indicator 'Critical Severity' with a checkmark, a status 'Confirmed', and a note '100+ affected assets in 10+ companies'. The main body of the alert describes threat indicators related to a variant of WannaCry (S0366) or WCry, which spreads as a worm through TCP port 445 (SMB) (T1018), exploiting the ETERNALBLUE SMB vulnerability (MS17-010) to encrypt files on the host, demanding a ransom to regain access (T1486). It also mentions that the threat can leverage another vulnerability known as DOUBLEPULSAR, which persists on compromised systems. The category is listed as 'Malware - ransomware'.

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



The screenshot shows a security alert for 'WannaCry'. The title is 'WannaCry' and the description is 'Disk encrypting malware contains worm-like features to spread itself using the SMBv1 ex...'. Below the title, there is a 'Critical Severity' dropdown menu with a checkmark, a 'Confirm' button, and a '+ companies' link. A tooltip is visible over the 'Confirm' button, displaying 'MITRE ATT&CK knowledge base' and 'Software: WannaCry'. The main body of the alert contains a paragraph of text: 'Threat indicators related to a variant of WannaCry (S0366) or WCry, a ransomware with worm capabilities wh... spreads as a worm through TCP port 445 (SMB) (T1018), exploiting the ETERNALBLUE SMB vulnerability (MS... encrypt the files on the host demanding a ransom in order regain access (T1486). Threat will attempt to conta... threat will stop its execution. Threat can also leverage another vulnerability known as DOUBLEPULSAR, a per... compromised systems.' Below this text, the category is listed as 'Malware - ransomware'.

...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

attack.mitre.org/software/S0366/

MITRE | ATT&CK[®] Matrices Tactics ▾ Techniques ▾ Mitigations ▾ Groups Softw

Search 🔍

Home > Software > WannaCry

WannaCry

WannaCry is ransomware that was first seen in a global attack during May 2017, which affected more than 150 countries. It contains worm-like features to spread itself across a computer network using the SMBv1 exploit EternalBlue.^{[1][2][3][4]}