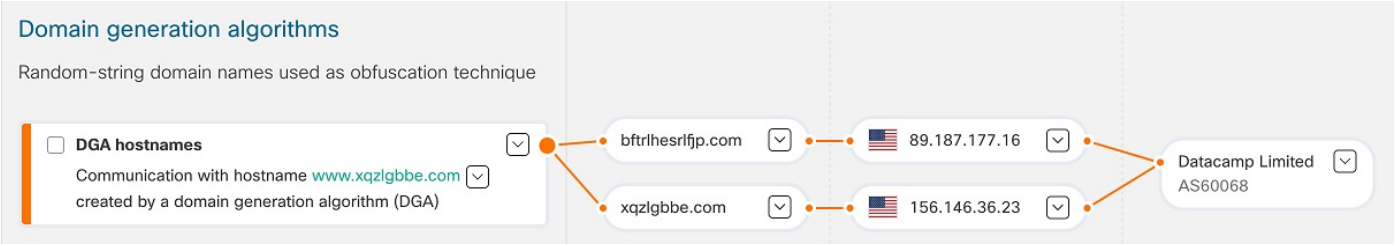
2021 年 4 月

2021 年 4 月にリリースされた、シスコのクラウドベースの機械学習によるグローバル脅威アラートに関するアップデートです。

新しい DGA 2.0 分類子

ドメイン生成アルゴリズム（DGA）は、攻撃者がホスト名をランダムに生成して、ブロッキング機能を備えたセキュリティ製品をバイパスするために使用されます。これらのアルゴリズムは、一般にボットネットやアドウェアの通信に使用されます。これらは動的に生成されるため、静的な署名ベースのウォッチリストに依存する、本来ならブロックする機能を果たすはずのセキュリティ製品がバイパスされてしまいます。

図 *1*：例：ブロッカーを難読化するために *DGA* によって生成されたランダム文字列ドメイン



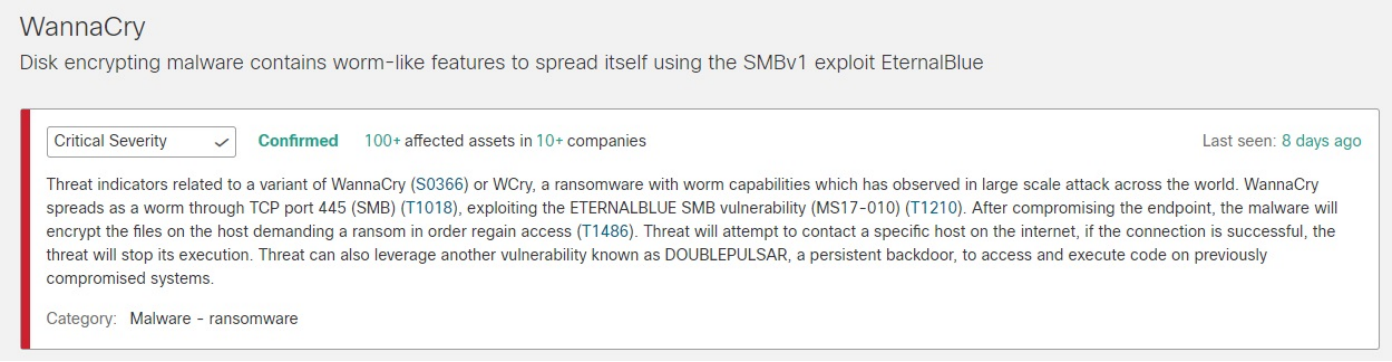
グローバル脅威アラートは 2015 年から DGA ドメインの検出をサポートしていますが、DGA 2.0 分類子は、古いランダムフォレストではなく、ニュートラルネットワーク（テキスト処理の最先端ソリューション）上に構築された新しいモデルです。このアーキテクチャの更新と新しく作成されたトレーニングセットにより、誤検出が少なくなり、再現率（偽陽性の数）が倍増しました。

これは、**[アラート（Alert）]**> **[アラート詳細（Alert detail）]**>**[セキュリティイベント（Security events）]** で確認できます。

アラートの説明で新しい MITER への言及

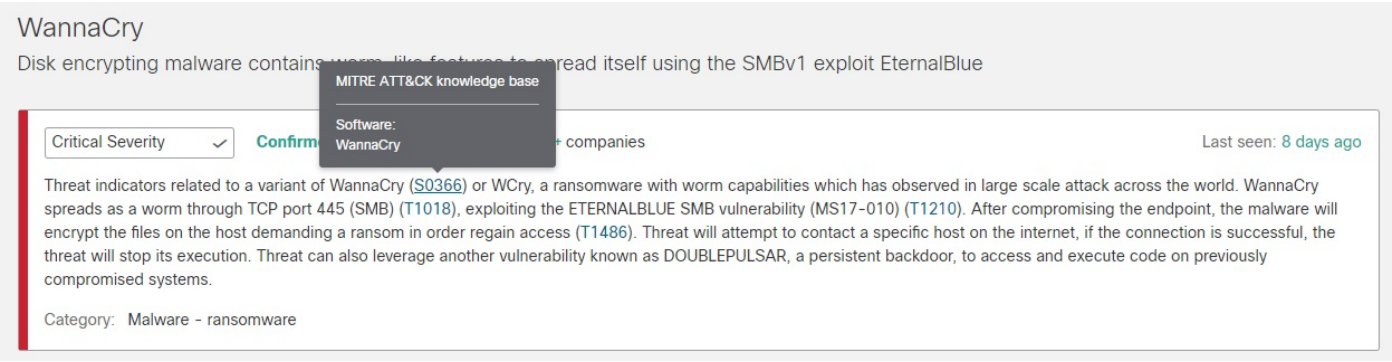
補足情報に簡単にアクセスできるように、MITER の参考資料をアラートの説明に直接追加しました。

図 *2 :* 例：*WannaCry* の説明内の *4* つの *MITER* 参考資料（*S0366*、*T1018*、*T1210*、*T1486*）



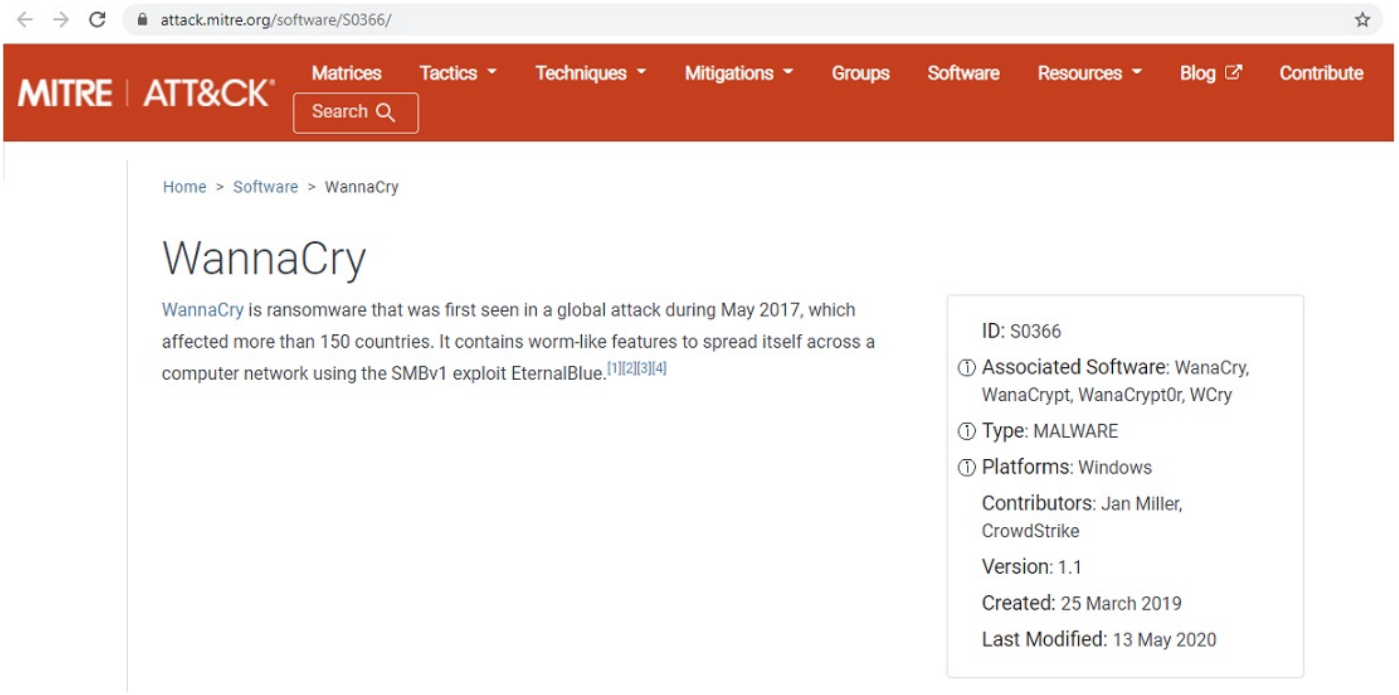
アラートやその説明に関する詳細情報を知りたい場合、ID 番号をクリックします。

図 *3 :* 例：*S0366* の *MITER ATT&CK* ナレッジベースへの埋め込みリンク



...新しいブラウザページが開き、MITRE ATT&CK のナレッジベースと特定の脅威に関する詳細情報が表示されます。

図 *4 : S0366* に関する詳細情報を示す *MITER ATT&CK* のページ



翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。