



2022 年 5 月

2022 年 5 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。

- [アラート詳細の拡張表示 \(1 ページ\)](#)

アラート詳細の拡張表示

[アラート詳細 (Alert detail)] ページを強化し、[影響を受けるアセット (Affected Assets)] に関する詳細情報を表示するようにしました。影響を受けるアセットにはそれぞれそのアセットで行われたすべての脅威検出をリストする新しい[脅威 (Threats)] セクションがあり、すべての有害となるセキュリティイベントが含まれています。

図 1:

Affected Assets

Username: **dusti.hilton** ETA

IP Addresses: **10.201.3.51**

Asset Groups: **Catch All**

Threats From: **2022-03-05 01:00:00 CET** To: **2022-05-31 06:14:58 CEST** Duration: **87 days**

- Emotet (S0367)** - Infection with exfiltration capability that targets banking credentials
 - Known malicious hostnames
 - Communication with hostnames **201.213.32.59** and **77.55.211.77** known to be indicative of **Emotet**
- WannaCry (S0366)** - Disk encrypting malware contains worm-like features to spread itself using the SMBv1 exploit EternalBlue
 - Known malicious hostnames
 - Communication with hostnames **www.iuqerfsodp9ifajaposdfjhgosurijfaewrwegwff.com** and **www.iuqerfsodp9ifajaposdfjhgosurijfaewrwegwea.com** known to be indicative of **WannaCry**
 - Known malicious hostnames from local passive DNS inference
 - Communication to IP addresses **104.16.173.80** with local passive DNS inference to hostname **www.iuqerfsodp9ifajaposdfjhgosurijfaewrwegwea.com** and **104.17.244.81** with local passive DNS inference to hostname **www.iuqerfsodp9ifajaposdfjhgosurijfaewrwegwea.com**. The hostnames are known to be indicative of **WannaCry**
- SMB service discovery (T1018)** - Discovery of external SMB servers, e.g. to exploit the ETERNALBLUE vulnerability
 - SMB protocol communication
 - Communication over SMB protocol with more than 5,000 IP addresses, hosted in more than 5,000 autonomous systems and 100 to 250 countries
- Excessive communication (T1498)** - Uniform communication to many external nodes
 - Excessive external communication
 - Connections to more than 5,000 IP addresses, hosted in 2,000 to 5,000 autonomous systems and 100 to 250 countries

> Contextual events From: **2022-03-05 01:00:00 CET** To: **2022-05-31 06:14:58 CEST** Duration: **87 days**

Asset Detail

[脅威 (Threats)] セクションの上部には、検出されたすべての脅威の合計観測期間と、特定のアセットでのそれらの有害となるセキュリティイベントが表示されます。

図 2:

Threats From: **2022-03-05 01:00:00 CET** To: **2022-05-31 06:14:58 CEST** Duration: **87 days**

それぞれの脅威検出には、その名前、MITRE リンク、説明、および以下のものが表示されます。

- 重大度

図 3:



- 観測期間

図 4:



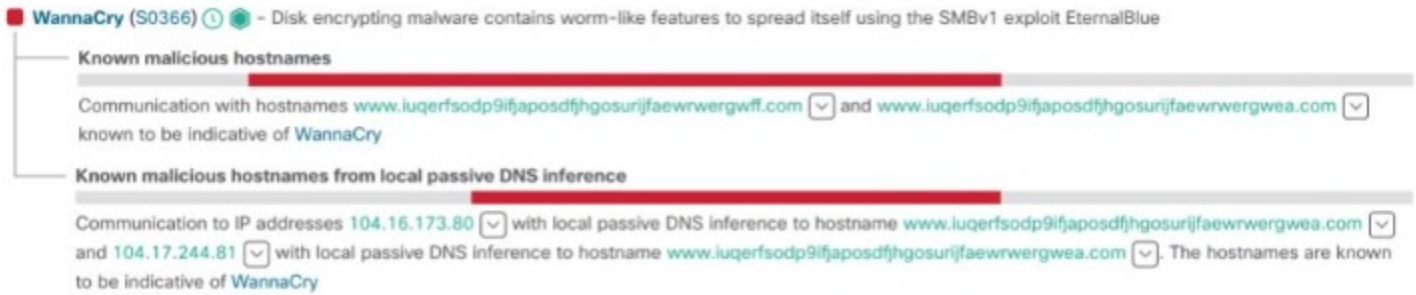
- 信頼度

図 5:



それぞれの脅威検出は、下にあるセキュリティイベントによって裏付けられています。イベントの多くには、イベントの作成につながった証拠を提供する豊富なセキュリティアナレーションが含まれています。

図 6:



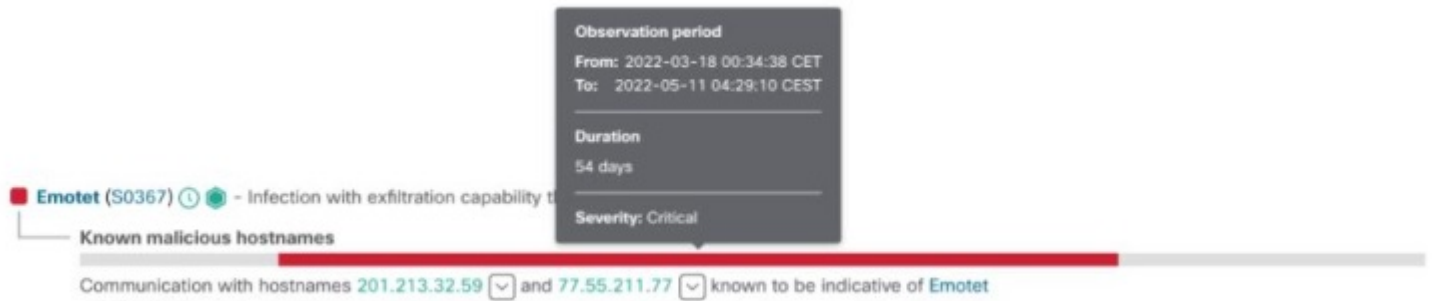
イベントアノテーションには、他のシスコのセキュリティ製品にピボットして、監視対象に関する追加情報とインテリジェンスを取り込めるドロップダウンメニューが含まれている場合があります。

図 7:



それぞれのセキュリティイベントには、[脅威 (Threats)] の合計観測期間のコンテキスト内での動作のタイミングと発生を示すタイムラインが含まれています。

図 8:



新しい [コンテキストイベント (Contextual events)] セクションを展開して、アセット上で起こったことに関する追加のコンテキストを提供できる、より多くのイベントを表示することができます。

図 9:



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。