



2022 年 4 月

2022 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。

- [MITRE ATT&CK® との調整 \(1 ページ\)](#)

MITRE ATT&CK® との調整

グローバル脅威アラートの脅威インテリジェンスレコードは、MITRE ATT&CK® フレームワークに関して調整されています。

- 必要に応じて、ATT&CK フレームワークからの命名が直接使用されます。
- グローバル脅威アラートの脅威インテリジェンスは、関連する ATT&CK の戦術、テクニック、およびソフトウェアエントリへの参照を提供します。

図 1:

Critical Risk	ETA
When:	February 5th - May 3rd
Modified:	yesterday
Threats:	WannaCry (S0366), Emotet (S0367), SMB service discovery (T1018), Excessive communication (T1498)
Asset Groups:	Catch All
Affected Assets:	2 assets
Username:	demo_keturah.gaunt, dusti.hilton
IP Addresses:	10.102.77.196 <input type="checkbox"/> , 10.201.3.51 <input type="checkbox"/>
	<input type="button" value="Accept"/> <input type="button" value="Reject"/> <input type="button" value="Alert Detail"/>

図 2:

SMB service discovery

Discovery of external SMB servers, e.g. to exploit the ETERNALBLUE vulnerability

High Severity



1,000+ affected assets in 100+ companies

Last seen: 2 days ago

Device is performing a scan of SMB services on TCP port 445 (SMB) (T1018), potentially to exploit the ETERNALBLUE SMB (MS17-010) or other vulnerabilities (T1210). Behavior is typical for variants of WannaCry (S0366) or WCry ransomware and unlikely to be legitimate, unless initiated by a user. To investigate, verify associated anomalies against intended behavior of the device.

Category: Attack Pattern - scanning

これらの改善により、インシデント対応の既存の標準操作手順とのプロセス統合が容易になり、新しいアナリストの学習曲線が短縮されます。

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。