サンプル

AEGISⅡ

防御証明ご報告書

2020年1月

株式会社ROCKETWORKS様

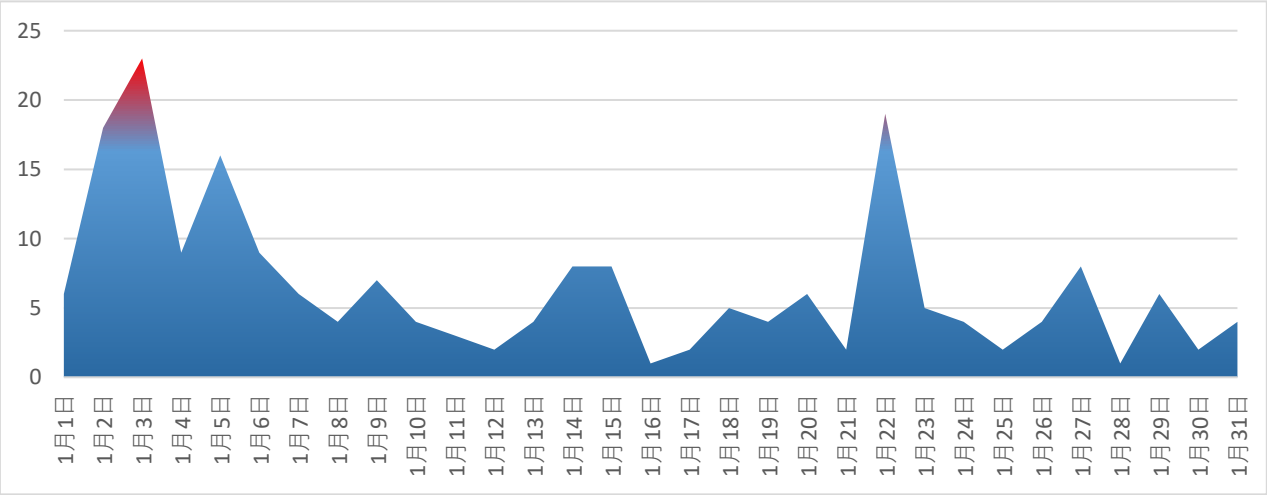
発行：株式会社ROCKETWORKS 東京都港区白金台3-18-1-3F

Rocketworks

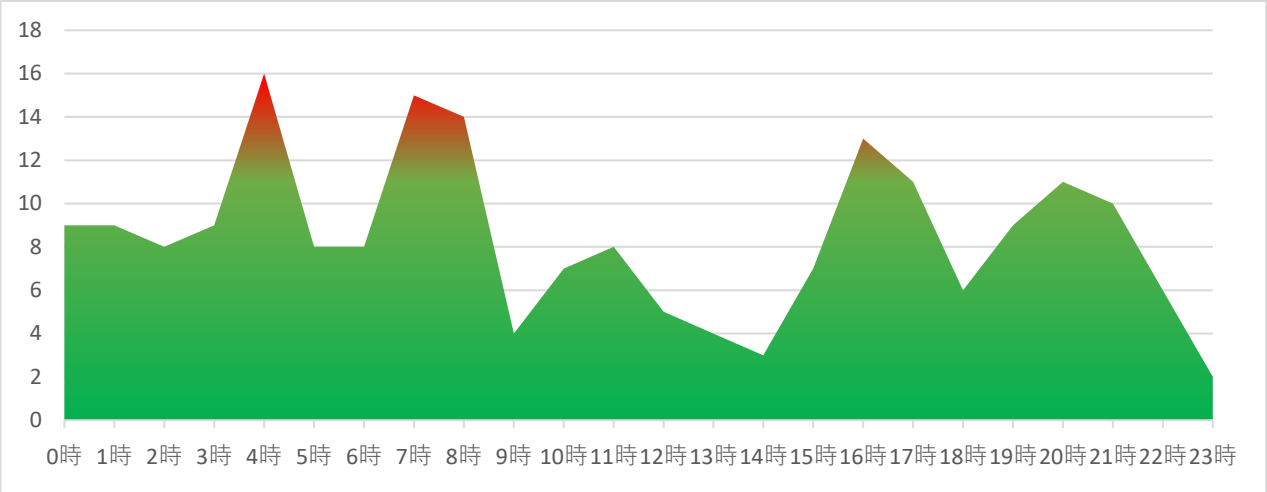
1.日別・時間帯別攻撃検出状況

全攻撃件数：202件

1-1.日別

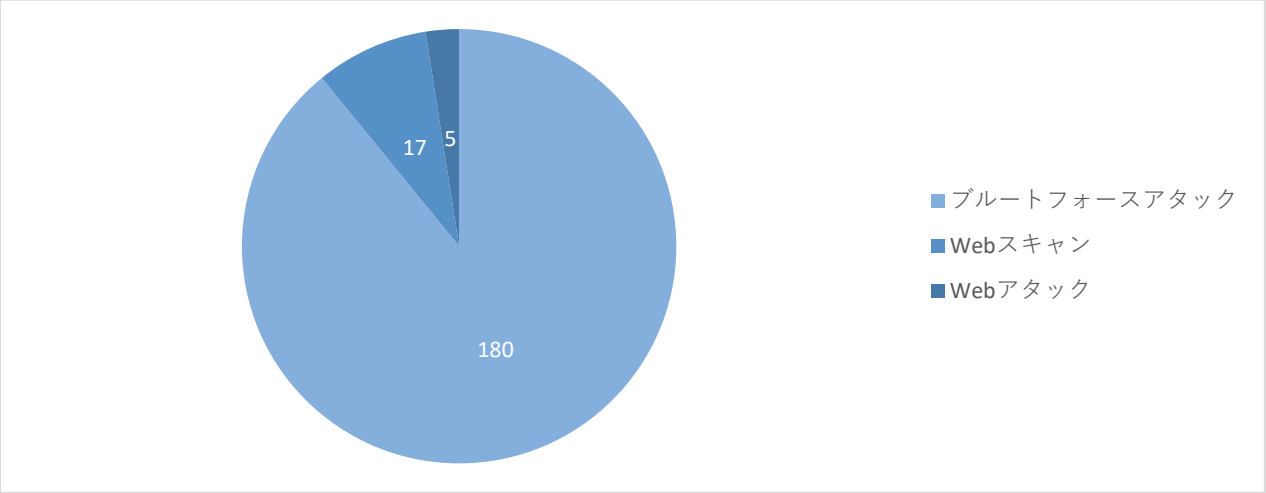


1-2.時間帯別



2.攻撃種別検出状況

全攻撃件数：202件

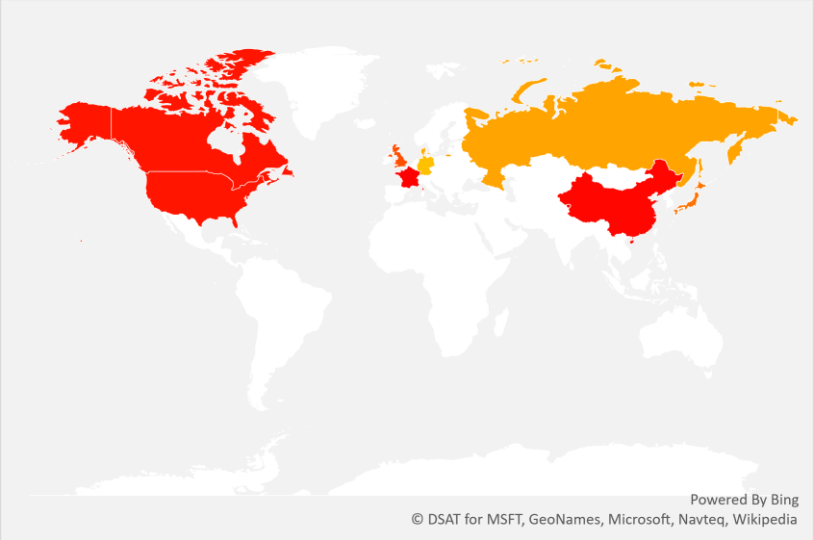


3.攻撃元別検出状況

全攻撃件数：202件

3-1.攻撃元ホストの地域（TOP10）

地域	件数
フランス	31
中国	30
アメリカ合衆国	28
カナダ	28
イギリス	20
日本	15
ロシア連邦	8
デンマーク	7
不明	5
ドイツ	4



3-2.攻撃元ホストのIPアドレス（TOP10）

IPアドレス	件数	地域	ホスト評価
62.4.XXX.XXX	11	フランス	スキャナー
51.254.XXX.XXX	10	イギリス	
178.33.XXX.XXX	7	フランス	
59.106.XXX.XXX	5	日本	
138.197.XXX.XXX	4	アメリカ合衆国	
212.114.XXX.XXX	4	ドイツ	
51.15.XXX.XXX	4	イギリス	
159.89.XXX.XXX	4	カナダ	
217.24.XXX.XXX	3	アルバニア	攻撃的ホスト
159.89.XXX.XXX	3	カナダ	

※ホスト評価…第三者調査機関により直近で攻撃的な活動が認められているホストです
　スキャナー：脆弱性の探索やアカウントの収集を行っている疑われるホスト
　スパマー：SPAMメールの送信元ホスト
　攻撃的ホスト：その他の攻撃的な行動が認められたホスト

4.総括レポート

全攻撃件数：202件

180件のブルートフォースアタックと17件のWebスキャン、5件のWebアタックを検出しました。

SSHによるサーバ接続を目的としたブルートフォースアタックを多数検出しました。公開鍵認証による接続に変更する、管理者の固定IPのみにアクセス制限をかける等の対策をおすすめします。

113.244.XXX.XXX（中国）ほかからは、不正に設置されたファイルを探索していると見られる活動が検出されました。すでに不正なアクセスを受けたサーバが対象となるため対応の必要はありません。ファイルのアップローダー等をサイト上に設置している場合、CMSやライブラリ等にアップロード機能が備わっている場合には、意図せず第三者にファイルをアップロードされないような設定を行ってください。

5.135.XXX.XXX（フランス）からはWebアプリケーションの脆弱性を幅広く探索する活動が繰り返し検出されました。Acunetix社製の脆弱性診断ツールを用いた情報収集目的の活動と見られます。お心当たりのない場合は、FW等での恒久的なブロックをおすすめします。社内や委託先による診断・調査の場合はホワイトリストへの登録の上、実施をお願いします。

120.26.XXX.XXX、139.224.XXX.XXX（中国）、46.101.XXX.XXX（ロシア）ほかからは大学図書館等で使用されている図書目録管理ツール（OPAC）を対象としたSQLインジェクション攻撃を検出しました。

92.101.XXX.XXX、178.69.XXX.XXX（ロシア）からはphpMyAdmin、SQLiteManagerといったWebインターフェースタイプのデータベース管理ツール対する探索行為が検出されました。これらのツールを利用されている場合は、Basic認証やIPアドレス規制等によるアクセス制限をおすすめします。またこれらWebアプリケーションのインストールスクリプト（setup.php等）の消し忘れ等も管理権限奪取等のリスクがあるためご注意ください。

182.48.XXX.XXX（中国）からはApache Tomcatを対象とした探索行為を検出しました。Tomcatでは一部コンポーネントについて過去に脆弱性が報告されています。使用されている場合はアップデート等のメンテナンスをおすすめします。