サンプル

AEGISⅡ

防御証明ご報告書

2022年2月

株式会社ROCKETWORKS様

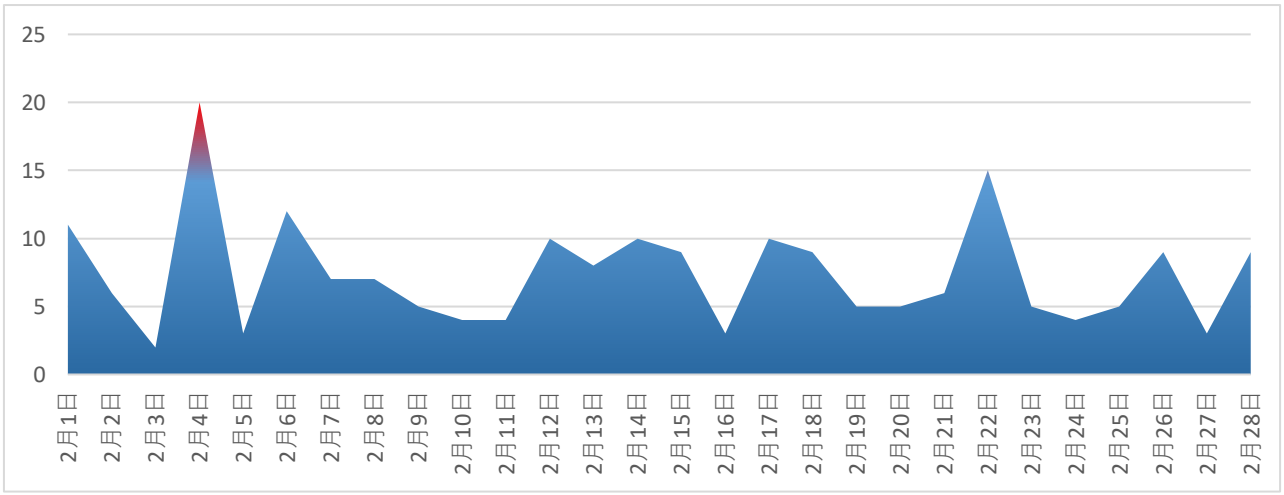
発行：株式会社ROCKETWORKS 東京都港区白金台3-18-1-3F

Rocketworks

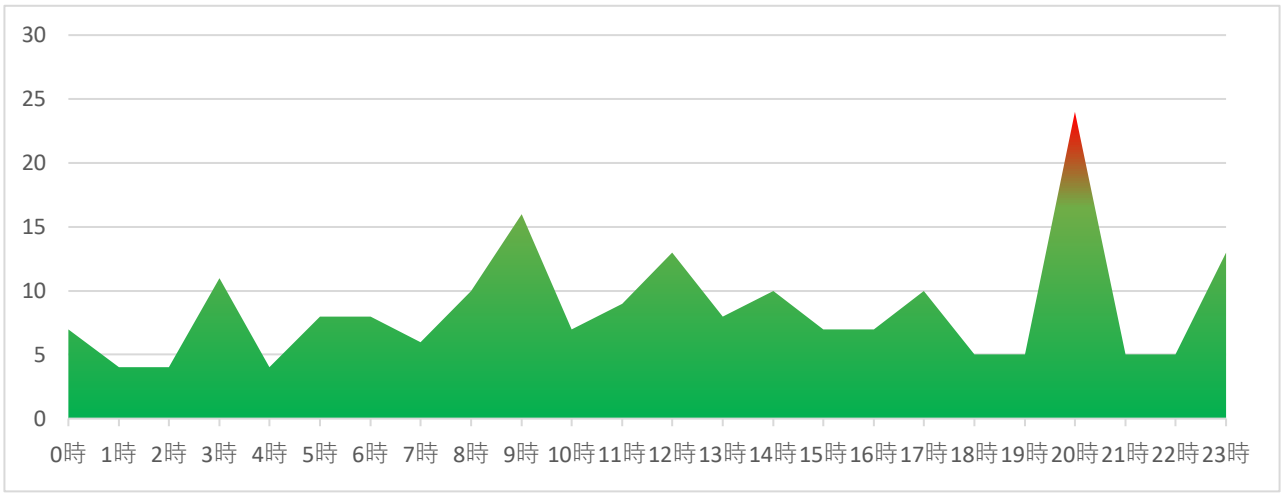
1.日別・時間帯別攻撃検出状況

全攻撃件数：206件

1-1.日別

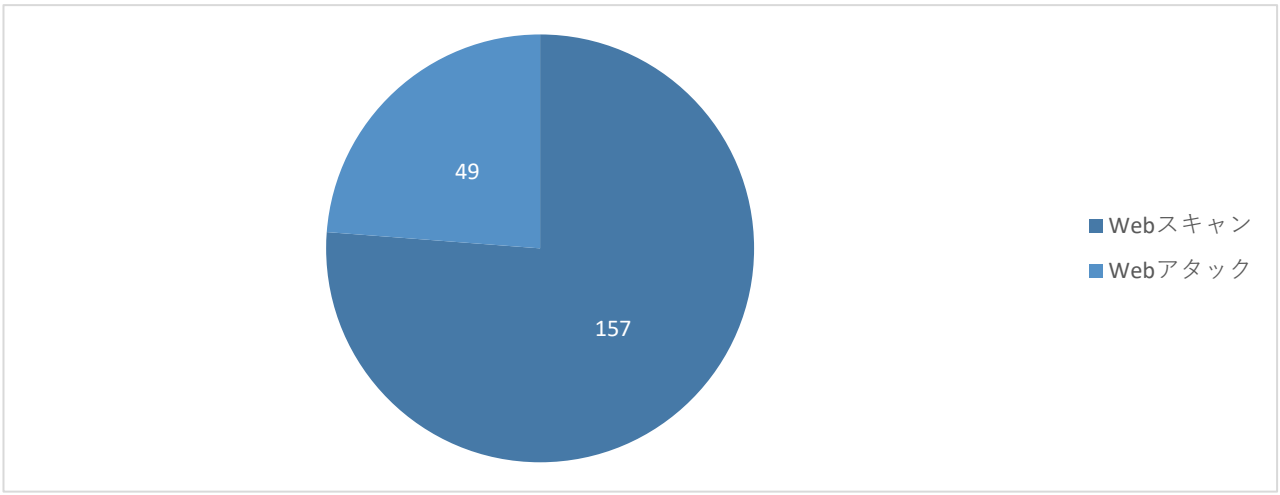


1-2.時間帯別



2.攻撃種別検出状況

全攻撃件数：206件

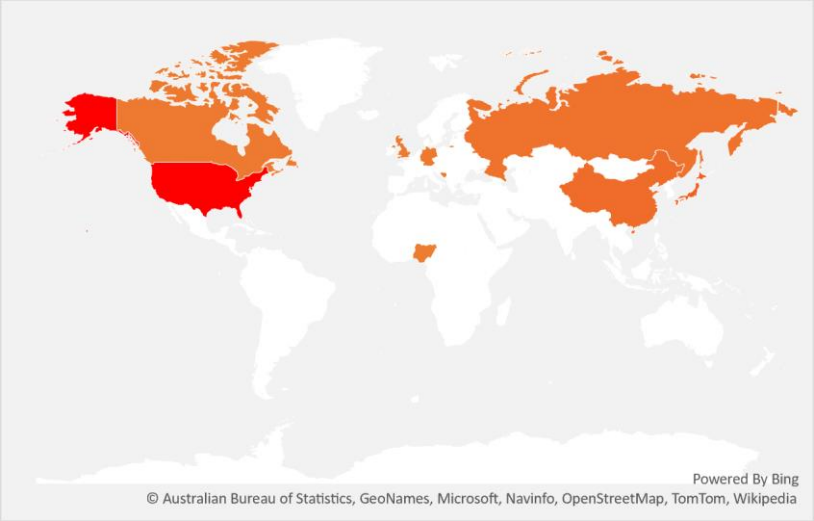


3.攻撃元別検出状況

全攻撃件数：206件

3-1.攻撃元ホストの地域（TOP10）

地域	件数
アメリカ合衆国	97
日本国	25
中華人民共和国	16
不明	14
ロシア連邦	11
ドイツ連邦共和国	6
ボスニア・ヘルツェゴビナ	5
イギリス	5
カナダ	5
ナイジェリア	3



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
52.68.XX.XX	9	アメリカ合衆国	
40.115.XXX.XXX	7	アメリカ合衆国	
20.214.XXX.XXX	7	アメリカ合衆国	
194.127.XXX.XXX	6	ドイツ連邦共和国	
100.25.XXX.X	5	アメリカ合衆国	
161.35.XXX.XXX	4	アメリカ合衆国	
95.181.XXX.XX	4	ロシア連邦	
18.206.XX.XX	4	アメリカ合衆国	
162.243.X.XXX	3	アメリカ合衆国	
183.150.XXX.XXX	3	中華人民共和国	

※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：206件

157件のWebスキャン、49件のWebアタックを検出しました。

52.68.XX.XX、40.115.XXX.XXX、20.214.XXX.XXX（アメリカ合衆国）ほかからの通信は、何らかの探索活動と見られますが、通信の内容からは特別に高いリスクは見受けられませんでした。他サイトへの攻撃実績から、サイトで使用されているアプリケーションの探索やマーケティングリサーチ（SEO調査や価格調査など）を行うロボットとみられます。

194.127.XXX.XXX（ドイツ連邦共和国）からは、SQLインジェクション試行が検出されました。過去に製造した機能等も含めて入力のエスケープが十分になされているかご確認ください。また普及率の高いアプリケーション（CMS等）やライブラリなどを使用されている場合は、バージョンアップ等、定期的なメンテナンスをおすすめします。

161.35.XXX.XXX（アメリカ合衆国）からはサーバのパスワードや権限奪取を目的としたディレクトリトラバーサル攻撃を検出しました。 とくに、Apache2.4.49, Apache2.4.50 については、ディレクトリトラバーサルの脆弱性が発見されております。脆弱性が悪用されると、アクセスが適切に制限されていないドキュメントルート外のファイルを第三者が読み取る可能性があります。また、CGIスクリプトにアクセス可能な場合、任意のコードを実行される可能性があります。各ディストリビューションの更新を適用するなどの対応をご検討ください。

95.181.XXX.XX（ロシア連邦）からは、オープンソースの脆弱性診断ツール「OpenVAS」を用いての脆弱性探索行為が検出されました。情報収集目的とみられますが、UserAgent名に「OpenVAS」が含まれる通信をWebサーバのモジュール等で制限することで一部抑制が可能です。

162.243.X.XXX（アメリカ合衆国）からは、オープンソースCMSのWordpressの脆弱性を持つプラグインやテーマの探索活動を検出しました。Wordpressを使用されている場合は、本体だけでなく、プラグインの更新も定期的に行ってください。またプラグインはメンテナンスが頻繁に行われているものを選定する、未使用のものや不要なものを削除するなど慎重な利用をおすすめします。

183.150.XXX.XXX（中華人民共和国）からは機微情報を含む静的ファイルの奪取を目的とした探索活動を検出しました。設定ファイルやバックアップ（ソースコード等）、SQLのダンプなどが対象となり、攻撃が成功した場合、サーバの乗っ取りや個人情報の漏洩のリスクがあります。～.confなど設定ファイルとして一般的なファイル名や.bak/org/old、.zip、.rarなどのファイルが総当りで探索されるため、これらのファイルを公開領域に放置しないようご注意ください。 また、アプリケーションがこれらのファイルを自動生成することがあるため、併せてご注意ください。