

【ニュースリリース】

2021年8月4日

報道関係者各位

サイバーセキュリティクラウド、2021年上半期の攻撃動向を調査した
「2021年1月～6月サイバー攻撃検知レポート」を発表
～増加する「SQLインジェクション」に注意～

株式会社サイバーセキュリティクラウド(本社:東京都渋谷区、代表取締役社長 兼 CEO:小池敏弘、以下「当社」)は、2021年上半期(2021年1月1日～6月30日)を対象としたサイバー攻撃検知レポートを発表いたします。なお、本データは当社が提供する、Webサイトへのサイバー攻撃を可視化・遮断するクラウド型WAFの「攻撃遮断くん」、AWS WAF、Azure WAFの自動運用サービス「WafCharm(ワフチャーム)」で観測した攻撃ログを集約し、分析・算出しています。

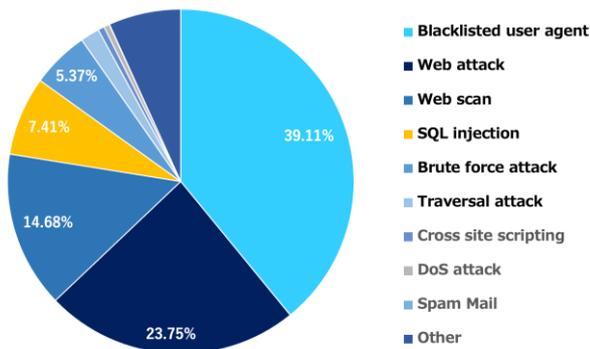
■調査概要

- ・調査対象期間:2021年1月1日～2021年6月30日
- ・調査対象:「攻撃遮断くん」、「WafCharm」をご利用中のユーザーアカウント
- ・調査方法:「攻撃遮断くん」、「WafCharm」で観測した攻撃ログの分析

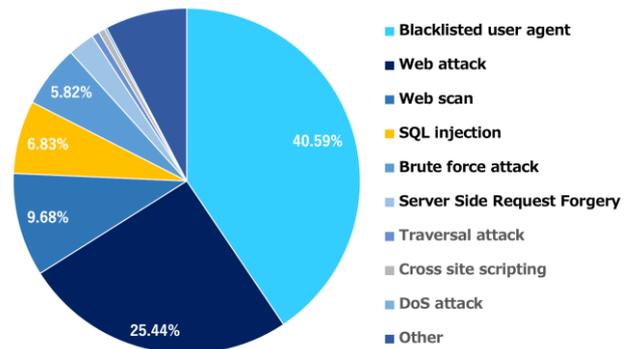
■攻撃種別ごとの検知数と攻撃動向

2021年の1月から6月の間において検知したサイバー攻撃の数は204,972,557件。これは10秒間で100件以上のサイバー攻撃を検知したことになります。

2021年1月～6月



2020年1月～6月



さらに検知した攻撃を攻撃種別ごとに分類すると、脆弱性スキャンツールなどを利用した Bot による攻撃である「Blacklisted user agent」が約 8,000 万件と、全体の 39.11% となる最も高い割合を占めました。次いで Web サーバーを構成するソフトウェアの脆弱性に対する攻撃である「Web attack」が約 4,800 万件で 23.75%、攻撃の対象を探索・調査したり、無作為に行われる単純な攻撃で脆弱性を探す方法である「Web scan」が約 3,000 万件で 14.68% と続きました。

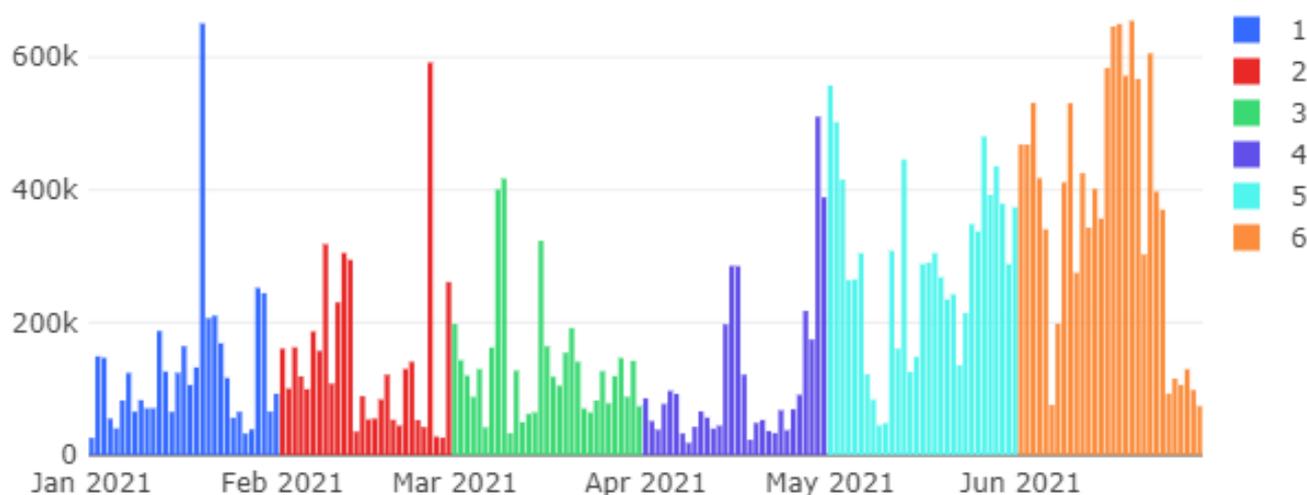
さらにシステムの脆弱性を意図的に狙い、想定しない SQL 文を実行させ、データベースシステムを不正に操作する「SQL インジェクション」が約 1,500 万件で第 4 位、総当たり攻撃とも呼ばれ、暗号や暗証番号に対して、理論的にあり得るすべてのパターンを入力して突破を試みる「Brute force attack」が約 1,100 万件で第 5 位となりました。

直接攻撃を仕掛けるのではなく、主に攻撃対象の探索を目的とする上位 3 種類の攻撃は数も多くなります。そうした攻撃の中でも本調査期間においては「Web scan」によって、攻撃の前にターゲットを探索する動きが強まっている特徴が現れていました。

一方で第 4 位の「SQL インジェクション」や 5 位の「Brute force attack」は、攻撃を通じて直接情報を窃取することを主な目的にしている攻撃です。中でも「SQL インジェクション」は前年同時期に比べ約 500 万件多く検知しています。こうした状況下において、サイバー攻撃への対策が十分でない企業がよりハッカーに狙われやすく、さらに集中して攻撃される可能性も高まっていると考えられます。

■主な脆弱性を狙った攻撃

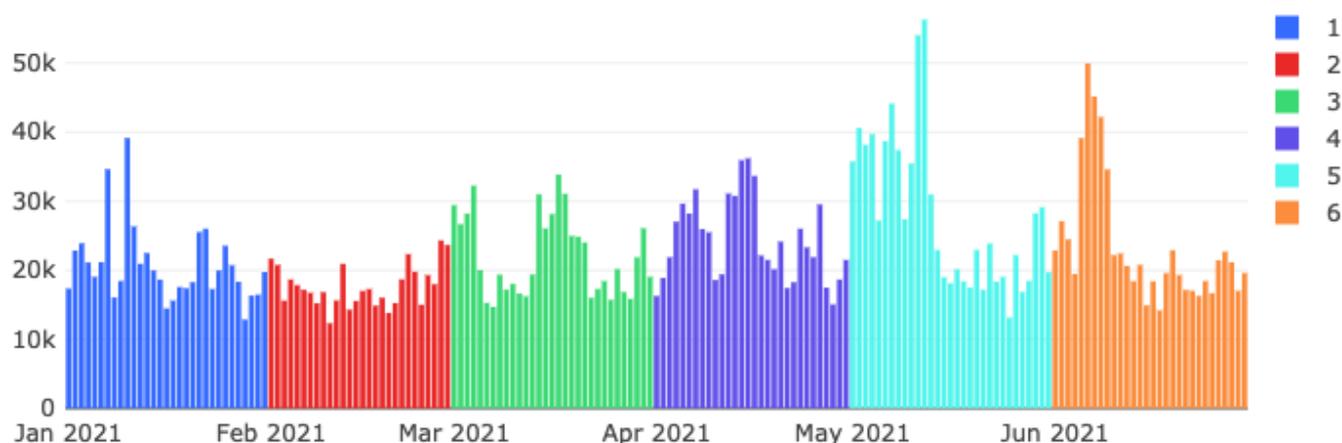
ー「SQL インジェクション」の攻撃検知推移



SQL インジェクションは、システムの脆弱性により本来意図しない不正な SQL が実行され、データベースが不正に操作される攻撃です。実際に攻撃を受けると、アカウントやクレジットカード情報の漏えい、不正サイトへの誘導やウイルス感染を目

的としたウェブサイト改ざんなどの被害が発生します。また国内では、6月に大規模な個人情報漏洩事案も発生しました。こうした中でWAFを導入している場合でも、定期的に脆弱性診断などの対策を強化し、脆弱性を作り込まないようにしていくことが重要になります。

一 WordPressの機能を拡張する各種「WordPress Plugin」の脆弱性を狙った攻撃



WordPressの機能を拡張する各種「WordPress Plugin」の脆弱性を狙った1日あたりの攻撃数が、1月から4月まではほぼ20,000~40,000の間で推移していたのに対し、5月前半に急激に増加しその後一旦落ち着いたものの、6月前半に再度急激に増加しました。5月以降に攻撃が増加している要因として、5月13日にWordPressのバージョン5.7.2が公開され、「PHPMailer」に対する脆弱性が見つかったことが考えられます。WordPressは便利な反面、攻撃されやすいことを十分に理解して今後もセキュリティ対策を万全にしておく必要があります。

【株式会社サイバーセキュリティクラウドについて】

会社名:株式会社サイバーセキュリティクラウド

所在地:〒150-0011 東京都渋谷区東 3-9-19 VORT 恵比寿 maxim3 階

代表者:代表取締役社長 兼 CEO 小池 敏弘

設立 :2010年8月

URL :<https://www.cscloud.co.jp/>

<本件のお問い合わせ>

株式会社サイバーセキュリティクラウド

経営企画部 広報 担当:竹谷

電話:03-6416-9996 FAX:03-6416-9997

E-mail:pr@cscloud.co.jp

サイバーセキュリティクラウド PR 事務局(スキュー内)

担当:北出・金子

TEL:03-6450-5457 E-Mail:csc@skewinc.co.jp