【ニュースリリース】

2023 年 8 月 10 日
株式会社サイバーセキュリティクラウド

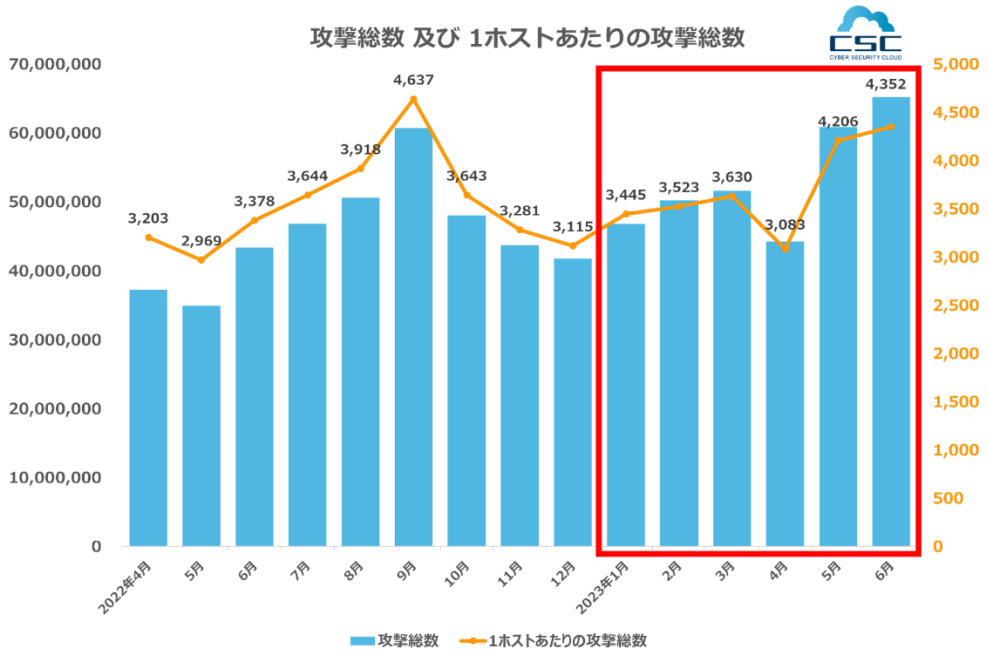
報道関係者各位

2023 年上半期 Web アプリケーションを狙った攻撃検知レポート
～TOP3 脆弱性に SQL インジェクションとクロスサイトスクリプティングがランクイン～

ハッカー対策サービスを展開するグローバルセキュリティメーカーの株式会社サイバーセキュリティクラウド（本社：東京都品川区、代表取締役社長 兼 CEO：小池 敏弘、以下「当社」）は、2023 年上半期（2023 年 1 月 1 日～6 月 30 日）を対象とした『Web アプリケーションを狙ったサイバー攻撃検知レポート（以下「本レポート」）』を発表します。
本レポートは、当社が提供する Web アプリケーション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』、及びパブリッククラウド WAF の自動運用サービス『WafCharm（ワフチャーム）』で観測したサイバー攻撃ログを集約し、分析・算出しています。

«レポートサマリー»
・2023 年 4 月～5 月にかけて攻撃が 138%に増加
・1 ホストあたりの SQL インジェクションが前年同期比で 110%に増加
・1 ホストあたりのクロスサイトスクリプティングが前年同期比で 220%に増加

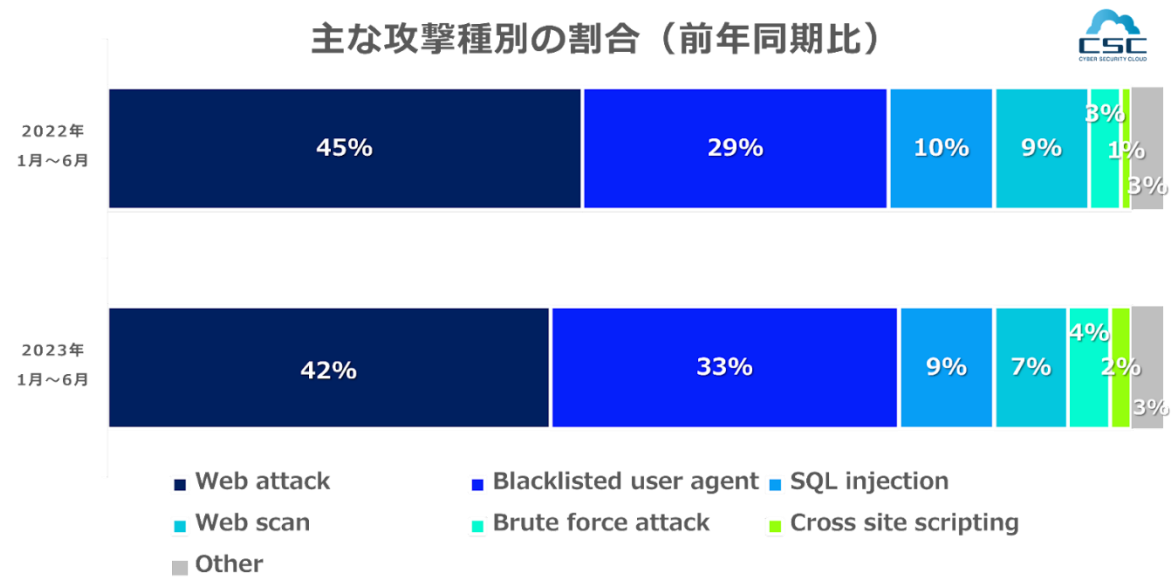
■ 2023 年 1 月～6 月のサイバー攻撃検知状況



2023 年 1 月 1 日～6 月 30 日までに、当社で検知した Web アプリケーションへのサイバー攻撃の総数は 319,001,684 件となり、1 ホストあたり（※）で 22,239 件でした。
さらに、当年比較では、2023 年 4 月から 5 月にかけて攻撃数が 138%に増加していることがわかりました。

世界規模で人が集まるイベントが開催されるとサイバー攻撃が増加する傾向にあり、5 月・6 月には G7 広島サミットや大臣会合という各国の首脳が集まるイベントが開催され、ウクライナのゼレンスキー大統領が急遽参加となったことも重なり、攻撃が急激に増加したと推測します。
※『攻撃遮断くん』の保護対象ホスト数（Web タイプ：FQDN 数、サーバタイプ：IP 数）と『WafCharm』の保護対象ホスト数（WebACL）との総数を分母に算出。

■ 攻撃種別



今回の調査期間における主な攻撃種別ごとの攻撃状況を見ると、主だった傾向は 2022 年上半期とさほど大きくは変わっていません。但し、脆弱性スキャンツールなどを利用した Bot による“Blacklisted user agent”は、2022 年 1 月～6 月とで比較すると 65,249,759 件から 101,953,562 件とおよそ 156%に増加していることから、次の攻撃対象を見つけるための偵察が活発化している可能性が考えられます。

■ Web アプリケーションの最大の脅威

研究開発を行っている米国の非営利組織 MITRE の調査結果（※）によると、ソフトウェアの最も深刻な脆弱性の中で、SQL インジェクションとクロスサイトスクリプティングが TOP3 にランクインしています。

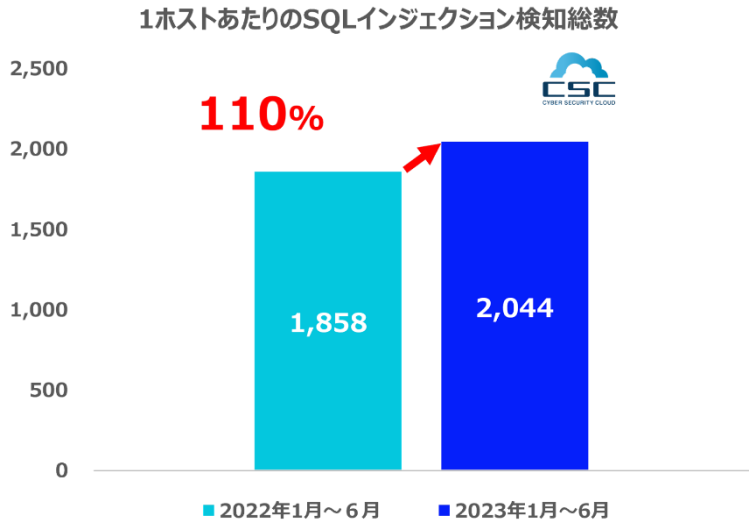
これらの脆弱性は、特に Web アプリケーションに対する深刻な脅威となります。開発者やシステム管理者は、適切な入力検証、アクセス制御、セッション管理などのセキュリティ対策の実装に注意を払うことが重要です。また、定期的な脆弱性診断やセキュリティ意識向上の取り組みも必要となります。

◆ SQL インジェクション

SQL インジェクションとは、外部からの入力を元に SQL 文を動的に作成するサイトやアプリケーションで、意図しない外部入力により悪意のある SQL 文を注入されることによって、不正にデータベースのデータが読み取られたり、データが改ざんまたは削除されたりする攻撃のことです。SQL インジェクションの脆弱性が悪用されると、外部からデータベースを操作され、その結果、データベースに記録されたデータの閲覧や盗難、変更、消去などが行われる可能性があります。

【本件に関するお問い合わせ】
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・川﨑
TEL：03-6416-9996 携帯:080-4583-2871(川﨑携帯)FAX：03-6416-9997
E-Mail：pr@cscloud.co.jp

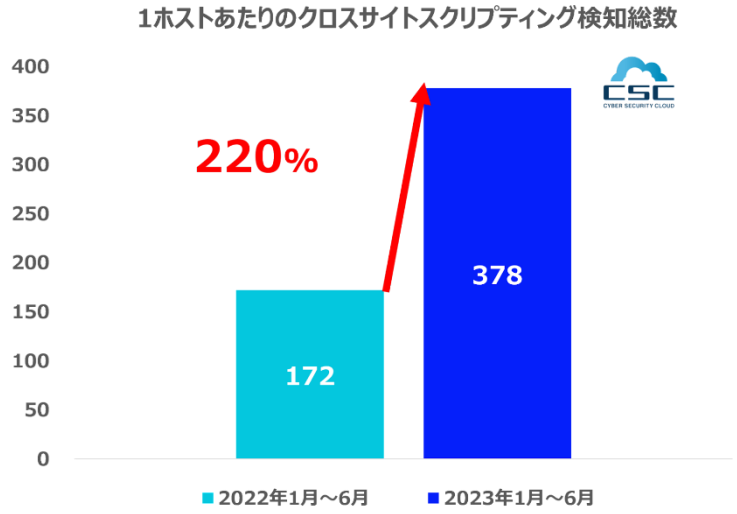
2022 年 1 月～6 月とで比較すると、2023 年 1 月～6 月の SQL インジェクションの攻撃総数は 22,451,970 件から 29,180,491 件とおよそ 130%（約 672 万件）に増加していることが分かりました。1 ホストあたりでは、1,858 件から 2,044 件と前年同期比でおよそ 110%に増加していました。



◆クロスサイトスクリプティング

クロスサイトスクリプティング（XSS）とは、Web サイトの脆弱性を利用し、記述言語である HTML に悪質のあるスクリプトを埋め込む攻撃です。アンケートサイトやサイト内検索、ブログ、掲示板などユーザーからの入力内容をもとに Web ページを生成するサイトや、Facebook、Twitter のような Web アプリケーションはクロスサイトスクリプティングの対象になりやすいです。サイトに設置されたフォームに攻撃者が用意したコードが埋め込まれた場合、ユーザーがそのフォームで情報を入力・送信する際、入力した情報に加え Cookie 情報や個人 ID なども攻撃者に送られます。これにより攻撃者は、被害者の SNS アカウントを乗っ取ったり、被害者の権限で社内システムに侵入したりできます。

2022 年 1 月～6 月とで比較すると、2023 年 1 月～6 月のクロスサイトスクリプティングの攻撃総数は 2,022,844 件から 5,396,930 件とおよそ 267%（約 337 万件）に増加していることが分かりました。1 ホストあたりでは、172 件から 378 件と前年同期比でおよそ 220%に増加していました。



【本件に関するお問い合わせ】
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・川﨑
TEL：03-6416-9996 携帯:080-4583-2871(川﨑携帯)FAX：03-6416-9997
E-Mail：pr@cscloud.co.jp

■ **長期休暇期間中のサイバー攻撃対策**

お盆休みなど、長期休暇期間は多くの組織でシステム管理者が不在となり、有事の際に迅速な対応が取れないケースが生じ易くなっています。また、PC 等を起動しない期間が長くなり OS や利用ソフトウェア等のアップデートが行われないため、休み明け業務を再開する際にウイルス等に感染する恐れもあります。被害を最小限に抑えるべく、長期休暇前後に全社員への対応通知を設定するなど事前の対策をお勧めします。

■株式会社サイバーセキュリティクラウドについて

住所　　：　東京都品川区上大崎 3-1-1 JR 東急目黒ビル 13 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/

サイバーセキュリティクラウドは「世界中の人々が安心安全に使えるサイバー空間を創造する」という経営理念を掲げ、世界有数のサイバー脅威インテリジェンスと AI 技術を活用した、Web アプリケーションのセキュリティサービス、及び脆弱性情報収集・管理ツールといったハッカー対策サービスを提供しています。これからも私たちは WAF を中心としたサイバーセキュリティにおけるグローバルリーディングカンパニーの 1 つとして、情報革命の推進に貢献してまいります。

■ **調査概要**

・調査対象期間：2023 年 1 月 1 日～2023 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アカウント
・調査方法：『攻撃遮断くん』『WafCharm』で観測したサイバー攻撃ログの分析

※ 出典：2023 CWE Top 25 Most Dangerous Software Weaknesses :
https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html

【本件に関するお問い合わせ】
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・川﨑
TEL：03-6416-9996 携帯:080-4583-2871(川﨑携帯)FAX：03-6416-9997
E-Mail：pr@cscloud.co.jp