【ニュースリリース】

2022 年 9 月 13 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

サイバーセキュリティクラウド、
昨今のサイバー攻撃情勢を承けて「サイバー攻撃検知レポート」を発表
～ロシアからの攻撃も加わり SQL インジェクション攻撃が期間平均の 3 倍に～

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」）は昨今のサイバー攻撃情勢を承けて、2022 年 8 月 1 日～9 月 8 日を対象とした Web アプリケーションへのサイバー攻撃検知レポートを発表したことをお知らせします。

尚、サイバー攻撃検知レポートのデータは当社が提供する 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。

■ 調査概要

・調査対象期間：2022 年 8 月 1 日～2022 年 9 月 8 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

■ 昨今のサイバー攻撃情勢

昨今、日本企業において、ロシアを支持するサイバー攻撃集団「キルネット」による「DDoS 攻撃」被害が相次いでいます。

DDoS 攻撃とは、攻撃の対象となる Web サイトやサーバに対して複数のコンピュータ等から過剰なアクセスやデータ通信を送信するサイバー攻撃です。DDoS 攻撃を受けることで通信のトラフィックが増大し、サーバに過剰な負荷がかかるため、サーバや Web サイトにアクセス出来なくなる等のサービス停止を引き起こします。

キルネットは日本国政府に向けて宣戦布告もしており、デジタル庁からも「当面は攻撃が続く可能性がある」と懸念されています。

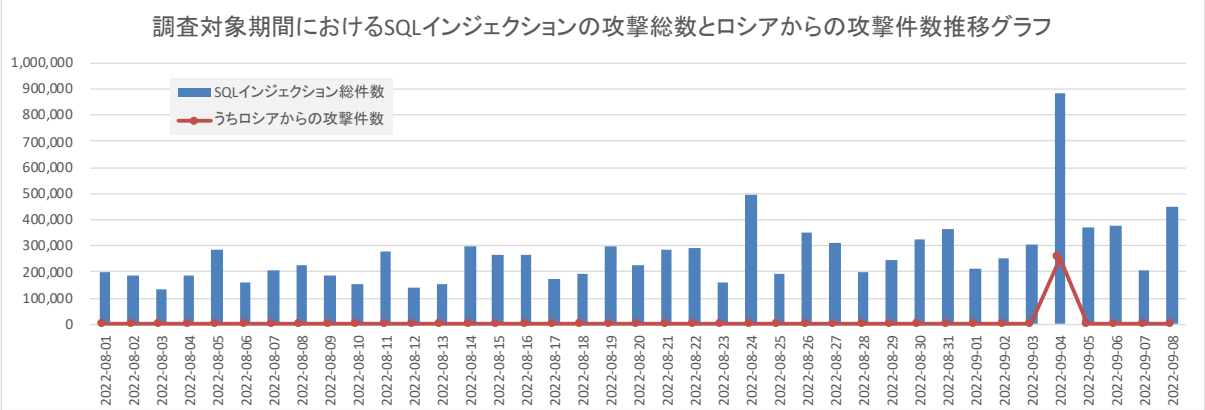
また本件との関連性は不明ですが、当社の検知ログ上で 9 月 4 日に SQL インジェクション攻撃が急激に増加していることが当社の調査で明らかになりました。

SQL インジェクション攻撃とは、Web アプリケーションの脆弱性を利用してデータベースを不正に操作する攻撃です。これは SQL という「データベースを操作する言語」を用い、脆弱性のある Web アプリケーション上の入力フォームなどに「不正な操作を行うための SQL 文」を意図的に「注入（インジェクション）」することで、データの窃取や消去、改ざん等を行うものです。

■ 攻撃種別ごとの検知数と攻撃動向

2022 年 8 月 1 日から 9 月 8 日までの 39 日間に当社で検知した Web アプリケーションへのサイバー攻撃の総数は 10,473,048 件でした。これは 1 分間に 186 件以上のサイバー攻撃を検知したこととなります。

特筆すべきは SQL インジェクションについて、対象期間の平均と比較して 9 月 4 日に約 3 倍となっている点です。また、調査期間においては、9 月 4 日のみロシアからの SQL インジェクション攻撃が観測されており、凡そ 29%を占めておりました。

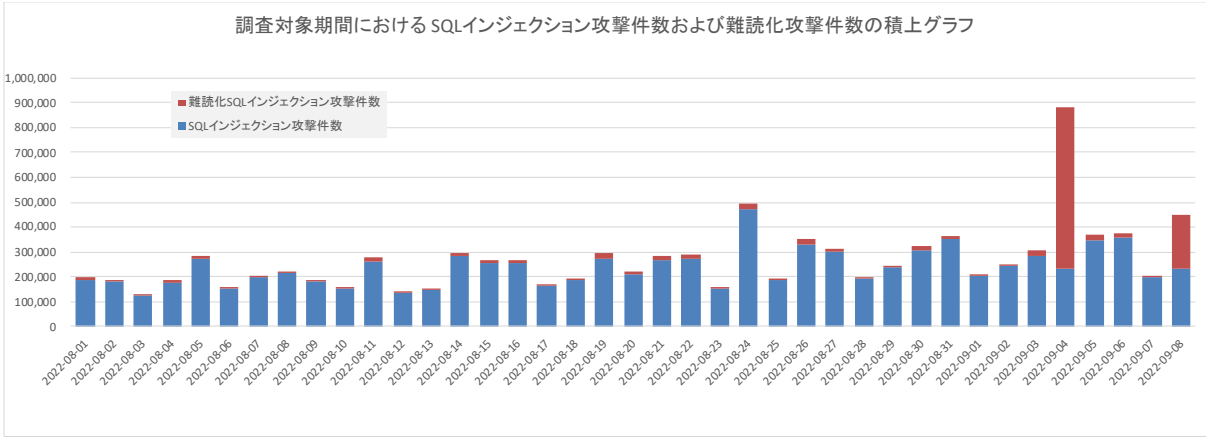


脆弱性を持つ Web サイトや EC サイト等が実際に SQL インジェクション攻撃を受けると、アカウントやクレジットカード情報の漏洩、不正サイトへの誘導やウイルス感染を目的とした Web サイト改ざんなどの被害が発生します。

■ 難読化された SQL インジェクションの増加

SQL インジェクションの攻撃内容に着目すると「難読化」された SQL インジェクション攻撃が増えていることが分かります。その割合について、通常時は約 5%程度ですが、9 月 4 日は約 70%と突出して増えています。

「難読化」とは、コンピュータプログラムの動作を変えずにプログラムを意図的に改変・加工して、人間視点での可読性を著しく下げ解析しづらくする技術です。本来はプログラムやアルゴリズムの改ざんやリバースエンジニアリング、盗用等を防ぐために用いられる技術ですが、ここでは恐らく攻撃の検知や解析などを遅らせる目的を持つと思われます。



直近、日本国内では 6 月に SQL インジェクションによって、大規模な個人情報漏洩事案も発生しました。かなり以前から用いられている攻撃であり、情報処理推進機構（IPA）『安全なウェブサイトの作り方』第一章の 1.1 に記載され、且つ別冊として『安全な SQL の呼び出し方』も発行されるほどです。セキュリティ実装の実施状況を確認するためのチェックリストも付属していますので、基本的な Web アプリケーションの脆弱性対応は必ず実施することを推奨します。

【株式会社サイバーセキュリティクラウドについて】
会社名：株式会社サイバーセキュリティクラウド
所在地：〒141-0021　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/
主な展開サービス：
- クラウド型 WAF『攻撃遮断くん』：https://www.shadan-kun.com/
- パブリッククラウド WAF の自動運用サービス『WafCharm』：https://www.wafcharm.com/
- 厳選された AWS WAF 用のルールセット『Cyber Security Cloud Managed Rules for AWS WAF』：
https://aws.amazon.com/marketplace/seller-profile?id=baeac351-6b7c-429d-bb20-7709f11783b2
- 脆弱性情報収集・管理サービス『SIDfm』：https://sid-fm.com/

【報道関係者からの問い合わせ先】
株式会社サイバーセキュリティクラウド PR 事務局（株式会社イニシャル 内）
担当：新貝・赤木・石坪・藤原
TEL：03-5572-7334
FAX：03-5572-6065
E-Mail：csc-pr@vectorinc.co.jp

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
TEL:03-6416-9996
FAX:03-6416-9997
E-Mail:pr@cscloud.co.jp