【ニュースリリース】

2022 年 8 月 9 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

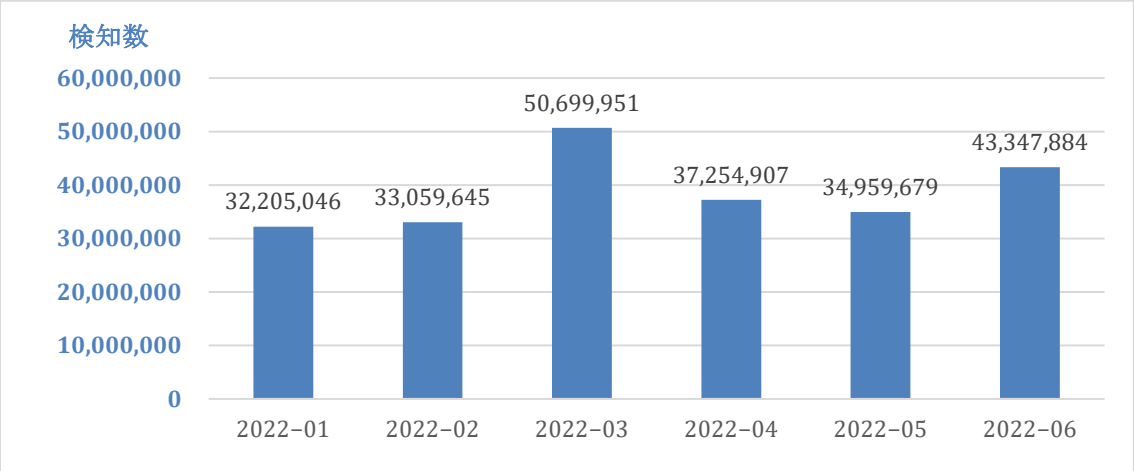
サイバーセキュリティクラウド、サイバー攻撃動向を調査した『2022 年上半期 Web アプリケーションへのサイバー攻撃検知レポート』を発表
～攻撃者が「準備フェーズ」から「攻撃フェーズ」へとシフトしている可能性～

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、2022 年上半期（2022 年 1 月 1 日～6 月 30 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いたします。
なお、本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。

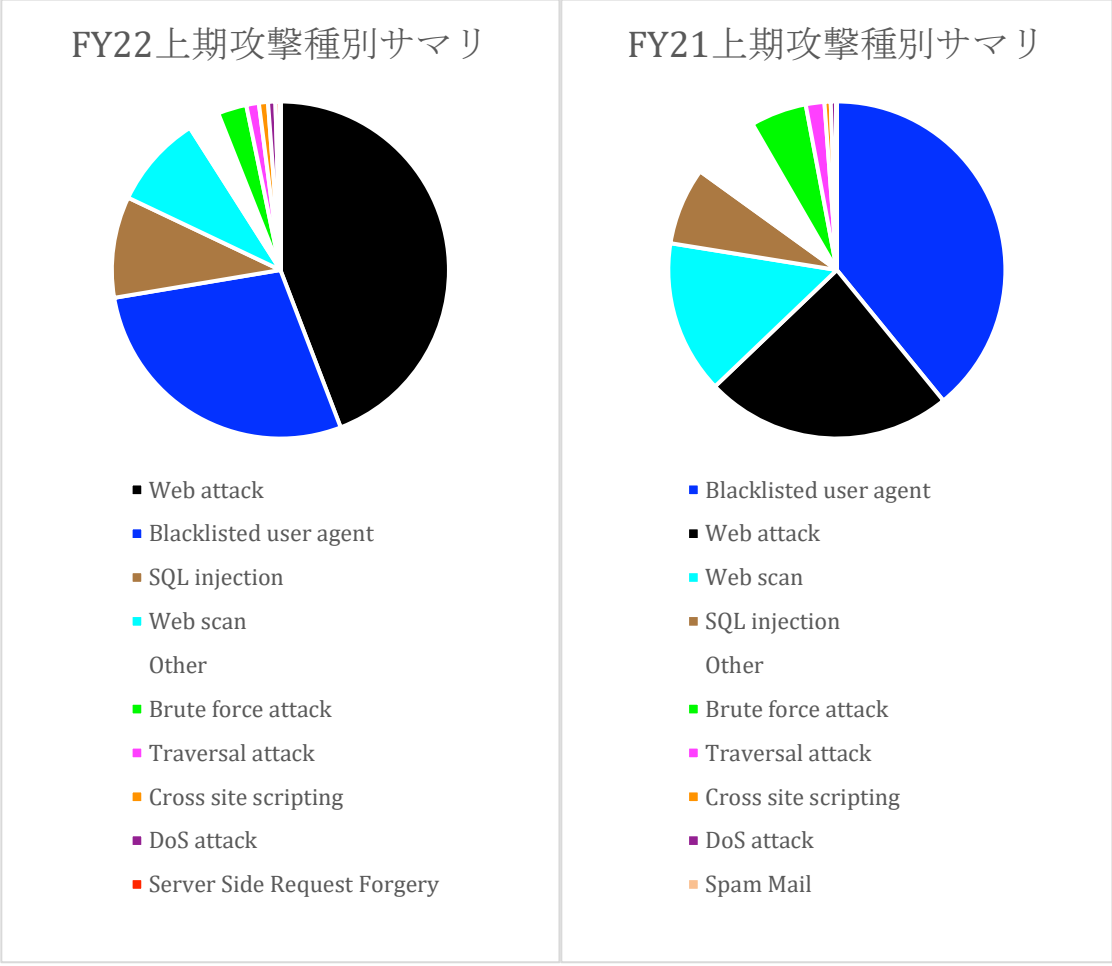
■調査概要
・調査対象期間：2022 年 1 月 1 日～2022 年 6 月 30 日
・調査対象：『攻撃遮断くん』『WafCharm』をご利用中のユーザアカウント
・調査方法：『攻撃遮断くん』『WafCharm』で観測したサイバー攻撃ログの分析

■攻撃種別ごとの検知数と攻撃動向
2022 年 1 月から 6 月までの 181 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 231,527,112 件。1 秒間におよそ 14.8 回のサイバー攻撃を検知した計算になります。

2022 年上半期 サイバー攻撃検知数



更に、当社が検知したサイバー攻撃を攻撃種別ごとに分類すると、2021 年上半期は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」がおよそ 8,000 万件と全体の 39%を超える割合を占めていましたが、2022 年では 2 位でおよそ 6520 万件、28%少々でした。今回最も観測数が多かったのは、2021 年上半期 2 位だった Web サーバ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」で、およそ 1 億 228 万件、割合としては全体の 44.18%と、2021 年の上半期の際と比べても倍以上の膨大な検知数へと増加しました。続いて 3 位が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」で、およそ 2,245 万件、9.7%でした。続いて、攻撃の対象を探索・調査し無作為に行われる単純な攻撃で脆弱性を探る「Web scan」がおよそ 2065 万件で 8.92%、となっていました。



category	total
Web attack	102,284,800
Blacklisted user agent	65,249,759
SQL injection	22,451,970
Web scan	20,653,889
Other	6,975,187
Brute force attack	6,386,266
Traversal attack	2,782,820
Cross site scripting	2,022,844
DoS attack	1,625,329
Server Side Request Forgery	952,604
XML External Entity	122,704
Spam Mail	13,563
Apache attack	5,259
Buffer overflow	118
総計	231,527,112

category	total
Blacklisted user agent	80,174,351
Web attack	48,674,751
Web scan	30,095,047
SQL injection	15,181,345
Other	13,754,051
Brute force attack	11,016,346
Traversal attack	3,658,184
Cross site scripting	1,224,400
DoS attack	1,070,077
Spam Mail	54,764
Server Side Request Forgery	34,549
XML External Entity	25,606
Apache attack	8,907
Buffer overflow	179
総計	204,972,557

本調査期間においては、Web サーバを構成するソフトウェア群の脆弱性を狙う「Web attack」による攻撃がかなり目立つ調査結果となりました。また、旧来から用いられている「主に脆弱性を利用して Web アプリケーションのデータベースに不正アクセスし、重要な機密データの窃取や改ざん、消去等の不正な操作を行う事を目的とする攻撃＝SQL インジェクション」の検知数は減少するどころか、2021 年下半期よりさらに 700 万以上増加しています。 実際に SQL インジェクション攻撃を受けると、会員のアカウント ID 情報やクレジットカード情報、会社の重要知財や独自ノウハウなど、そこに保存されている重要な情報の窃取や改ざん、消去、また Web アプリケーションの改ざんによる不正サイトへの誘導やマルウェア感染などの被害が発生します。

■攻撃者が「準備フェーズ」から「攻撃フェーズ」へとシフトしている可能性

SQL インジェクションとは、Web アプリケーションのデータベースを不正に操作する攻撃手法で、主な攻撃対象は会員制サイトなど「データベースを使って重要情報を管理している Web アプリケーション」つまり「Web アプリケーションの運営元企業」です。

なお、SQL インジェクションの中にも技術的にいくつかの種類に分けられます。

- インバンド SQL インジェクション：Web アプリケーションへの入力に対するレスポンスを元に脆弱性などを調査分析し、発見された脆弱性を元にして不正な SQL 文を注入し攻撃する手法です。

- エラーベース SQL インジェクション：意図的に Web アプリケーションにエラーメッセージを出力させて、そこから脆弱性などを調査分析し、発見された脆弱性を元にして不正な SQL 文を注入し攻撃する手法です。

- ブラインド SQL インジェクション：複数の SQL 送信に対する応答ページの違いを確認し、そこからデータベース管理システムに関する情報を窃取＝応答ページだけを見てもその攻撃に気付くことは困難なため、対策を怠ると大変な被害に拡大するまで全く気付けないこともあります。

他にもマルチプルステートメント、UNION インジェクションなどの手法があります。

同様に Web アプリケーションを狙った攻撃手法として名前が挙がるものに「クロスサイトスクリプティング（XSS）」があります。こちらはデータベースの有無は直接関係なく、脆弱性のある Web アプリケーションに悪意のあるスクリプトを仕込み、その Web アプリケーションに触れた利用者の端末にてスクリプトを実行、ユーザを攻撃者の偽 Web サイトに誘導（＝クロスサイト）する（もしくは遷移させずその場で不正なスクリプトによる情報の窃取などを実行する：最近このパターンが増えている）攻撃手法です。XSS が SQL インジェクションと大きく異なるのは、直接の攻撃対象が「標的の Web アプリケーションを利用するユーザ」だという点です。

これらの攻撃によって発生する被害者はサービス運営元企業だけでなく、直接的な被害の主体は窃取された情報の所有者、つまりサービス利用者です。そして彼らにとって、預けた情報を盗まれたり悪用されたりといった害を被った際、彼らにとっての直接的な加害者が「サービス運営元企業」となる可能性が非常に高くなります。

こうした攻撃手法の検知が 2021 年下半期から継続的に増加傾向にあるということは、単純に直接攻撃を仕掛けてくるケースが増加しただけでなく、これまで潜伏調査していた攻撃者がこれまでの準備期間で、つまり調査目的のアクションで得た様々な対象の情報を元に、徐々に攻撃フェーズへとシフトしつつある可能性も否定できません。

■我々が現在直面している世界情勢について

2022 年上半期は特に、国際的かつ大規模な社会情勢の変動、それに伴う経済の不安定化など、私たちの生活にも大きく影響する出来事が発生し、それは今もなお続いています。こうした不安定な情勢も手伝って、2021 年 1 月にテイクダウンしたはずのマルウェア『Emotet』の復活と過去に例を見ない拡散、様々な深化・変化を起こしている亜種の登場は極めて大きな脅威として、日本を含め世界中で今猛威を揮っています。

またランサムウェアについても、相変わらず極めて攻撃規模は大きく、特に今年は中小企業が標的とされた事例が多く目立ちます。ダークウェブ上では、こうした攻撃が安価かつ簡単にセット～実行できるツールやソリューション、攻撃代行サービス等が販売されていて、いわばカジュアルな攻撃とでも呼ぶべきものが増加の一途を辿っています。現代は誰もが容易に高度なサイバー攻撃を実施できる時代と言っても過言ではない時代です。

従来のセキュリティ対策、そしてその延長となるエンドポイントセキュリティや SOC などによる監視はどちらかというと何かが起こったことに検知＝「事後調査」の意味合いが強く、マルウェアには有効でもランサムウェア対策には不十分です。何故ならば、ランサムウェアは身代金目的にしても破壊目的にしても「業務を停止させる」攻撃ですので、当事者として最優先すべき事項である『業務再開』には、監視はあまり貢献しません。こうした脅威には「事前の準備」＝「なってしまう・起きてしまう前提での実態を反映した対策」が必要不可欠になるわけです。

■最後に

長期休暇の時期には、IPA（情報処理推進機構）等からも注意喚起が行われているようにシステム管理者が長期間不在になるケースもあり、何かあった際の対処が遅れる可能性もありますので、有事の際の対応フロー、機器やデータ持ち出しに係る休み期間中の特別ルール策定など、長期休暇前に事前準備はしっかり整えておきましょう。

また休み明けについて、長期休暇中に電源を落としていた機器には、その間にメーカー等からアップデートが用意されている場合が多くあります。そうした修正プログラムの適用・定義ファイル更新などにはシステム管理者等の指示に従って適宜対応しましょう。ただし、アップデートを装うポップアップ等でマルウェアをインストールさせよう等と企てる攻撃者も少なくないため、それが偽物である可能性を踏まえて、アップデート等はポップアップ等に従って操作することなく、機器やソフトウェア等にそれぞれ正規の手順でのアップデートを行うよう注意した方が良いでしょう。

同様に、休み明けは不審なメールも多く届いているケースは多く、本文中の URL でフィッシングサイトへ誘導される、またマルウェア感染するなどの可能性があるため、まず基本として添付ファイルや記載の URL には触らず、システム管理者等にまずは対応方法を確認して指示に従うよう周知徹底しましょう。

現代は「誰もが容易に攻撃者になり得る」時代で、国家のような大きな組織同士のサイバー戦争なども当たり前になりつつあります。今後、自分は攻撃されない前提で考えることを止めて、自分も当事者だという自覚を持つことと、最低限の防御が可能となるように事前理解と準備が大切になります。デジタルが当たり前に存在することが前提の DX 社会で、セキュリティ後進国のみならずデジタル後進国とさえ言われてしまう日本を今後「もっと便利でセキュアな国」にしていくためにも、私たち一人一人のこうした心掛けはますます強く意味を持っていくと思います。

【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/

【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：深田・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