【ニュースリリース】

2022 年 11 月 21 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

2022 年度第 3 四半期の「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
～1 秒間に 20 回程度のサイバー攻撃を検知～

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、2022 年度第 3 四半期（2022 年 7 月 1 日～9 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 7 月 1 日～2022 年 9 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

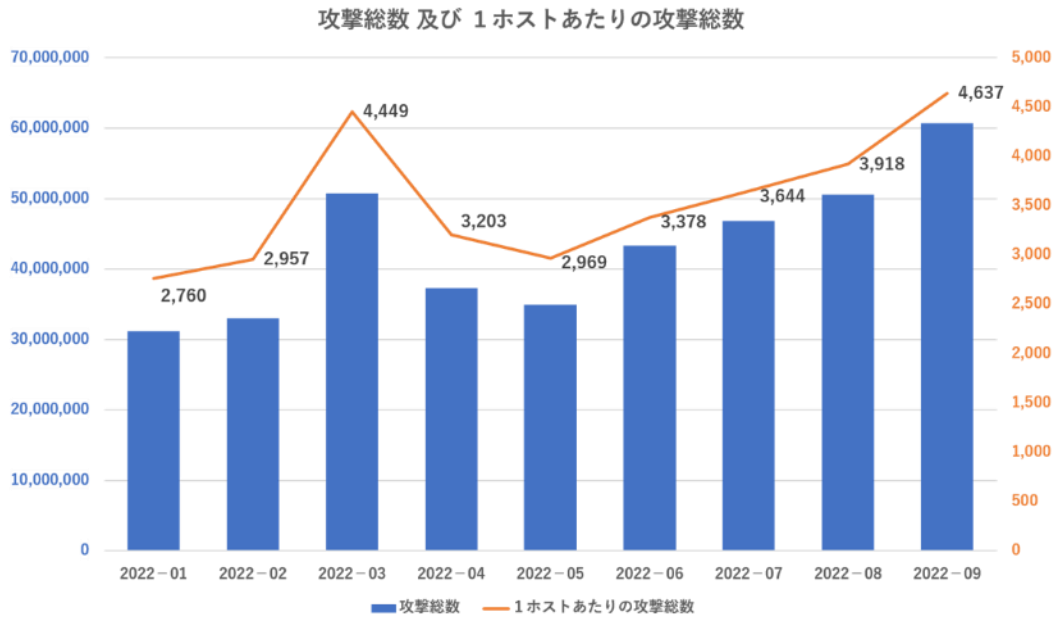
■ 昨今のサイバー攻撃情勢：サプライチェーン攻撃が目立つ

昨今、不安定な国際情勢の影響を受けてか、日本国内においても様々なサイバー攻撃被害、特にサプライチェーンを狙ったサイバー攻撃などの被害が相次いで目立っています。サプライチェーン攻撃については、商品が製造される過程において一社単独で行われることは極めて少なく、原料や部品の調達から組み立て、梱包、流通など様々な企業の一連の繋がり（これがサプライチェーンと呼ばれる）が存在することを利用した攻撃手法です。そうしたサプライチェーンの中に存在する様々な企業、グループ企業や製品の部品製造業者、物流業者など様々な関連企業の中で「情報セキュリティ関連の対策が弱い企業」を見つけ出し、攻撃する手法を指します。

■ 検知総数と推移：1 秒間に 20 回程度のサイバー攻撃を検知

2022 年 7 月 1 日から 9 月 30 日までの第 3 四半期に、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 158,181,684 件でした。これは 1 秒間に 20 回程度のサイバー攻撃を検知していることとなります。月別に見ると、7 月度は 46,852,025 件、8 月度が 50,602,450 件、9 月度は 60,727,209 件となっており、大きく右肩上がりとなっています。なお、この傾向は半年近く続いています。

また、これを 1 ホスト当たりで見ても、7 月度は 3,644 件、8 月度は 3,918 件、9 月度は 4,637 件となっており、全体的に大きく右肩上がりであることが分かりました。



こうした傾向はここで収まるとは限らず、これまでの傾向、また年末年始を狙う攻撃者も毎年一定数存在することなどを踏まえると、今後もこの右肩上がりの傾向は暫く続くと考えられます。こうしたサイバー攻撃の増加に備え、改めて境界防御が包括的に実施されているかどうかを確認すること、そして自組織の持つあらゆる情報資産について棚卸しし、それぞれに対応策を漏れなく定め、適用管理することをお勧めします。

■ 攻撃元・攻撃種別：2022 年度上半期からの大きな変化はない

また当該期間のサイバー攻撃について、攻撃元 IP アドレスを国別に見ると、1 位が米国、2 位が日本国内、続いてカナダ、フランス、ドイツ、ロシアと続きました。

ただ以前から、特に大掛かりな組織が標的型攻撃を仕掛ける場合は直接ターゲットにではなく、途中に様々な国のデータセンターなどを幾度も経由し、相手から本当の攻撃発信元の所在地を知られないようにカモフラージュすることも非常に多くなっています。また攻撃を数十分から数時間で実施完了、その間だけサーバを用意し、攻撃行為が終了するとすぐにダウンさせるケースも少なくありません。

そして攻撃種別については、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」が 1 位で変わらずおよそ 7,100 万件、そして未だに「SQL インジェクション攻撃」がおよそ 2,370 万件強と 3 位、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 810 万件少々と 4 位に位置していました。

2022 年度上半期（2022 年 1 月 1 日～6 月 30 日）からの変化という意味では、特に目立った変化はないように感じられます。

■ 社会全体を見渡して：目立つ「サプライチェーン攻撃」と「ビジネスメール詐欺（BEC）」

この四半期については、他にも国内への DDoS 攻撃についてはやはり特に目立った増減などは見られない状況でした。またお気づきの方も少なからずいらっしゃるかもしれませんが、日本国内においては国際情

勢で騒がれるようないわゆるハクティビストやサイバー軍といった「信条・己の正義感」を満たす目的での攻撃関連よりも、やはり営利（金銭）目的などの攻撃が目立ったように思います。

特にここ最近で目立っていると感じる攻撃につきましては、先にも挙げたサプライチェーン攻撃と、BEC（ビジネスメール詐欺）が挙げられると思います。

■ サプライチェーン攻撃：サプライチェーン全体でのセキュリティ対策を

前述した「サプライチェーン攻撃」は大きく分けて 2 つの攻撃に分けられます。まず一つ目は、ターゲットに定めた企業の製品サプライチェーンを構成する関連企業（原材料やパーツなどの仕入れ先や発注先等々）を調べて、セキュリティ対策が不十分な対象を発見し、そこへの攻撃を足掛かりにしてターゲット企業に侵入したり、ターゲット企業の機密情報を関連企業から窃取したりといったものです。

もう一つの攻撃はソフトウェアサプライチェーン攻撃とも呼ばれます。現状は製品の製造において機能別のパーツ（ハードウェア／ソフトウェア）を購入し、それらを組み合わせて IT 機器やソフトウェア製品を完成させることが一般的ですが、そのパーツ等にマルウェアを仕込んだりバックドアを仕込んだりしておく方法や、製品アップデートファイルやパッチなどにマルウェアを仕込むものです。この場合は製品の消費者が直接の被害者となるケースが多く、被害としてはより広い範囲に影響を及ぼし、より大きな問題に発展する可能性もあります。

独立行政法人情報処理推進機構（IPA）の『サイバーセキュリティ経営ガイドライン』には、経営者が認識すべき「3原則」の中に「自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要」と明記されています。今や自社だけの対応で安心するのではなく関連企業全体、サプライチェーン全体のセキュリティ対策が求められていると強く認識し、対応を図り、継続的に管理運用し、定期的な見直しと改善を続けることが必要です。

■ ビジネスメール詐欺：「違和感」にいち早く気付くことが重要

BEC（ビジネスメール詐欺）とは「電子メールに巧妙な細工を施して取引先や役員になりすまし、企業の担当者を騙して金銭を振り込ませるサイバー攻撃」と定義されています。特に IT リテラシの低い、かつ手続き上の権限を持っている相手を狙って、極めて判別が困難な偽のメールを送付し、ターゲットをだまして金銭を搾取する、というのが主だった攻撃パターンです。

例えばターゲットの取引先のメールシステムに侵入して、習慣的に送信されている毎月の請求書 PDF の「振込先だけ」を攻撃者の海外銀行口座等に改ざんし「取引先のメールサーバ」から正規に送信します。この際、本物のメールはターゲットの受信トレイに届かないよう細工します。担当者がその改ざんに気付かずに「攻撃者」にお金を振り込んでしまい、取引先からの入金督促があって初めて発覚、振込先の銀行に問い合わせても既にお金は引き出されてしまっていた、といったようなケースは典型的なパターンかつ被害額が大きいものの一つだと思います。

BEC への対策は、担当者個人の範疇では「注意」すること、違和感にいち早く気付くこと、例えば「いつもの銀行口座じゃない」とか、元から時々振込先が変わる取引先であっても「何で海外の口座に振り込むのだろう」とかを考えることが重要です。組織では担当者個人だけで完了するようなオペレーション／ワークフローにはせず、処理対応の途中で関わる誰かが気付けるような冗長体制を作ることが重要です。

IPA にはビジネスメール詐欺（BEC）対策特設ページ（https://www.ipa.go.jp/security/bec/）が存在し、2022 年 9 月に更新・追記が行われました。また同じく IPA サイトにビジネスメール詐欺の事例集（https://www.ipa.go.jp/security/bec/bec_cases.html）もあり、こちらも 2022 年 10 月に更新・追記が行われています。これらも参考に対策を進められることを強く推奨します。

■ **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/

　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。

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

■ **報道関係者のお問い合わせ先**

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