News Release

報道関係者各位

ニュースリリース

平成 31 年 1 月 31 日

株式会社サイバーセキュリティクラウド

【サイバー攻撃白書　2018 年度攻撃分析レポート発表】
「攻撃遮断くん」で検知した攻撃ログ数は約1億件超
企業規模を問わないサイバー攻撃の検知を観測

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：大野　暉、以下「サイバーセキュリティクラウド」）は、2018 年のサイバー攻撃の実情についてまとめた、「サイバー攻撃白書 2018」を発表いたします。

「サイバー攻撃白書」とは、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」で観測した攻撃ログを集約し、分析・算出した調査レポートです。

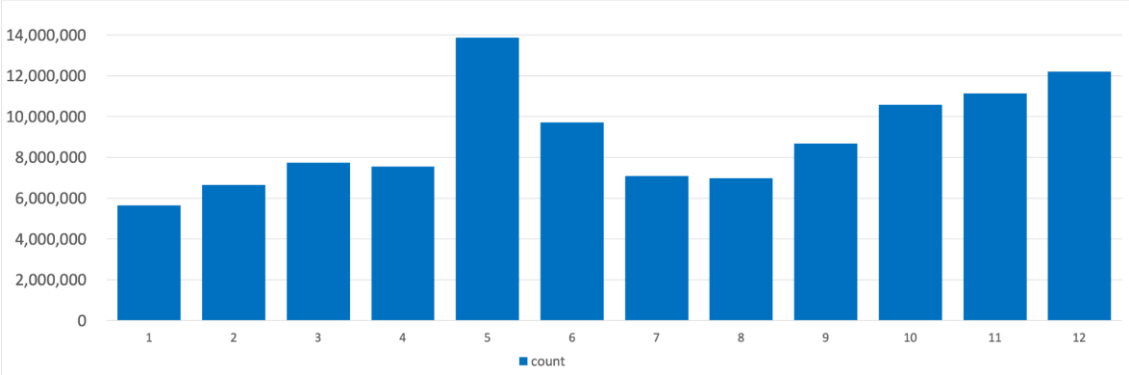
本レポートを公開していくことで、各業界の企業に対してサイバーセキュリティに関する意識喚起を行ってまいります。

■「2018 年度　サイバー攻撃白書」概要

-調査対象期間　：2018 年 1 月 1 日（月）～2018 年 12 月 31 日（月）
-調査対象　：「攻撃遮断くん」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」で観測した攻撃ログの分析

■2018 年の攻撃状況

2018 年の導入企業への攻撃ログ数は合計 107,803,890 件となりました。月単位で1番多く観測されたのは 5 月となっております。また、2018 年は後半にかけて月ごとに攻撃数は多く観測されており、今後も攻撃ログ数が増えていくことが予想されます。

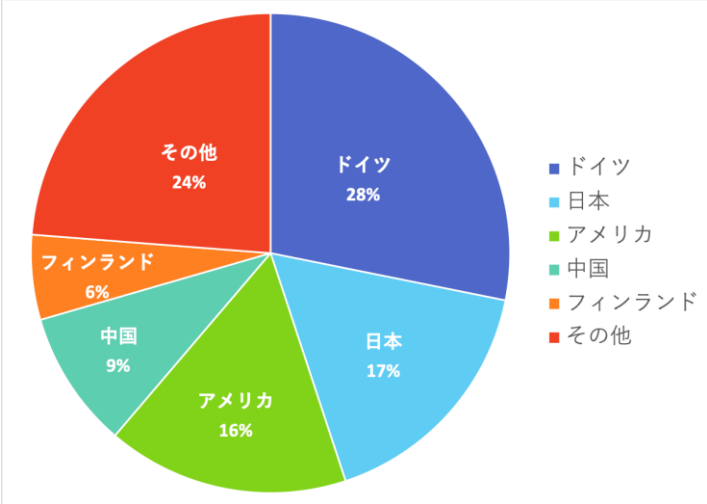


年間攻撃数推移

■攻撃元の国別の割合

2018 年に検知した攻撃の攻撃元 IP アドレスを国別に集計したのが、下記のグラフです。

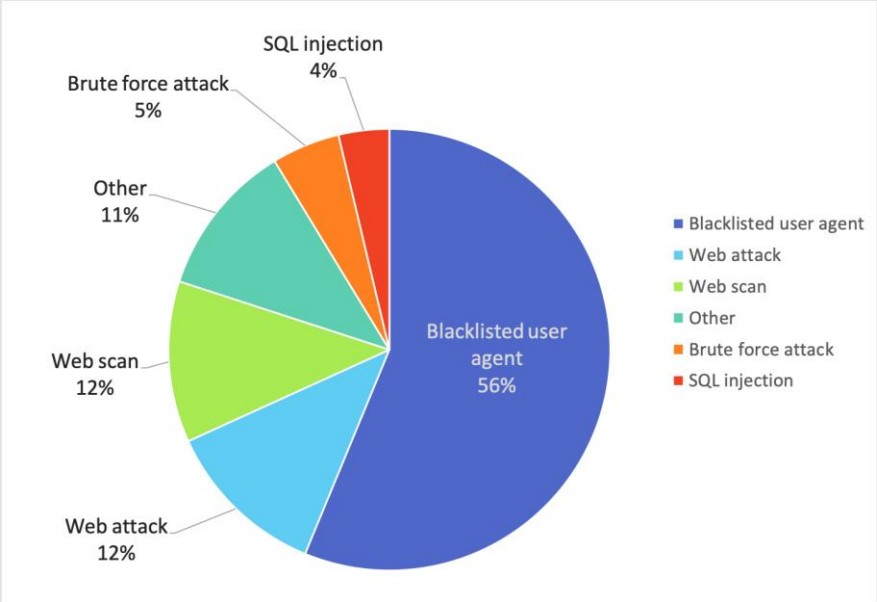
クラウド型 WAF「攻撃遮断くん」導入サービスにおける、攻撃元の国別 Top 10 の1位はドイツとなりました。それぞれの順位とパーセンテージは、1 位:ドイツ(28%)、2 位:日本(17%)、3 位:アメリカ(16%)、4 位:中国(9%)、5 位:フィンランド(6%)となっております。



攻撃元の国別の割合

■攻撃別の構成比

下記は検知した攻撃種別の構成比を現したグラフです。攻撃全体の 56%が「Blacklisted user agent」によるものとなり、突出していることが読み取れます。



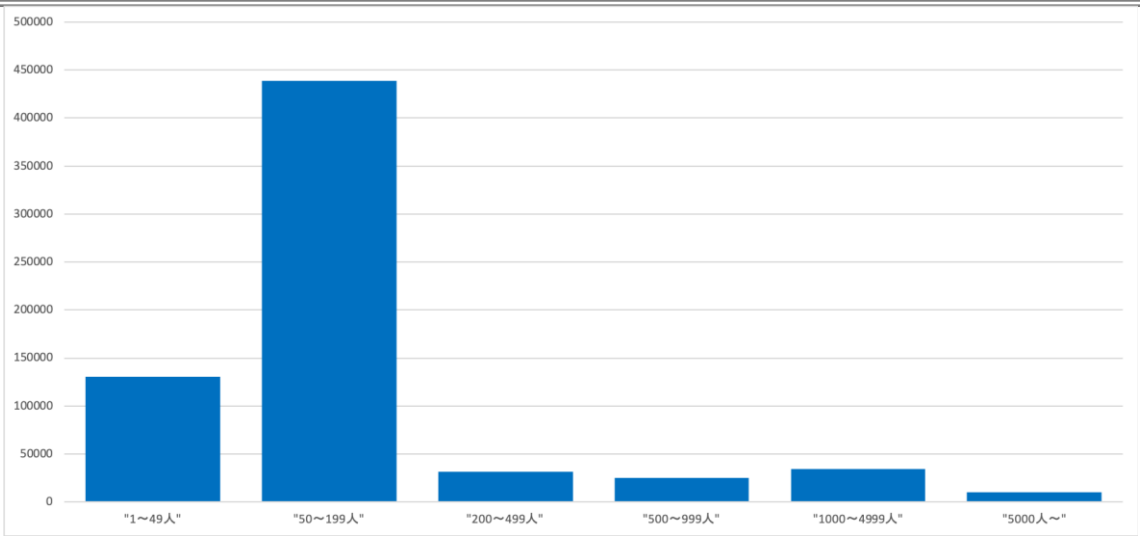
■Blacklisted user agent について

全体の約 60%を占める「Blacklisted user agent」とは脆弱性スキャンツールを利用した Bot による攻撃を検知したものです。

「Blacklisted user agent」として検知するスキャンツールの1つである「ZmEu」は 2012 年 9 月ごろに開発されたツールではありますが、依然攻撃の手段として利用されています。このツールは phpMyAdmin の脆弱性をスキャンします。Web サーバの安全を確保するためにも、最新のバージョンへアップデートする必要があります。

■企業規模別の平均攻撃検知数

以下のグラフは、企業規模で分類した1社あたりの攻撃検知数の平均グラフです。50～199 人規模の企業への攻撃がもっとも多く観測されています。1～50 人規模の企業や 5,000 人規模の企業への攻撃も計測されていることから、前述した Blacklisted user agent（脆弱性スキャンツールを用いた Bot による攻撃）をはじめとした様々なサイバー攻撃の脅威に、企業規模に問わずさらされていることがわかります。



企業規模別の平均攻撃検知数

■攻撃概要

1.Blacklisted user agent

脆弱性スキャンツールを利用した Bot による攻撃です。

「ZmEu」「Nikto」「Morfeus」などといったスキャンツールが該当します。

2.Web attack

DoS 攻撃に近いものや OS コマンドインジェクションを行う攻撃です。

3.Web scan

攻撃の対象を探索・調査する動作や、無作為に行われる単純な攻撃で脆弱性を探す攻撃予兆と見られる方法です。

4.Brute force attack

暗号解読やパスワードを割り出すために総当たりで攻撃する方法です。

5.SQL injection

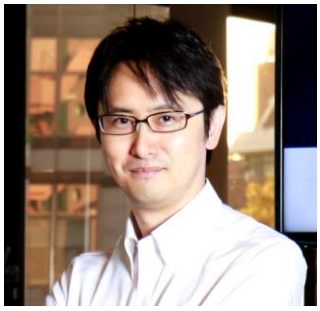
WEB アプリケーションの脆弱性を利用し、アプリケーションが想定してない SQL 文を実行させることで、DB を不正に操作する攻撃です。

6.Other

上記に記載した攻撃手法の他にも、クロスサイトスクリプティングやディレクトリトラバーサルなどの攻撃方法がありますが
比較的割合が少なかったものについては Other としています。
各種 OS やミドルウェアなどの脆弱性を突いた攻撃などや通常、WAF の範囲外とされるものなども含みます。

■専門家コメント（総括）

株式会社サイバーセキュリティクラウド　取締役 CTO　渡辺　洋司



2018 年　の Web セキュリティを振り返りますと、3 月には、Drupal(Drupalgeddon 2.0) のセキュリティホールが見つかり大きな話題となりました。この脆弱性は昨今話題の仮想通貨のマイニングを動作させるための準備にも使われており、攻撃の目的が多様化していると言えます。
Web アプリケーションに関するフレームワークでは、Struts2, Tomcat, Spring, WebLogic　に関する脆弱性も報告されており、該当するかどうかの調査・判断や、アップデートの対応可否の判断などに追われたのではないでしょうか。

リモートコードが実行可能となるセキュリティホールは攻撃者の目的に応じたプログラムを動作させることが可能となっており、コインマイナーに関する調査やプログラムの配備などは 2018 年の特徴的なものであったと言えます。1 年を通してみると WebScan と呼称している、サーバーのファイル構成などを調査する攻撃の検知数も増大しており相関性が伺えます。

脆弱性が発見されるプログラムにはサポート切れとなっているものも存在しておりこの様な場合にはセキュリティアップデートが存在せず対応が困難となります。
また、サポートされているバージョンであってもアップデートの対応には時間がかかるものです。
攻撃の目的は多様化しており、個人情報の窃取が目的でないケースも増えてきておりますので、個人情報の有無や企業規模に関わらず Web サイトを保有する組織は、サーバーの監視と対策の重要性は高まっていると言えます。

■「攻撃遮断くん」について

https://www.shadan-kun.com/

「攻撃遮断くん」は、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 Web セキュリティサービスです。
官公庁や金融機関をはじめ、大企業からベンチャー企業まで業種や規模を問わず様々な企業で採用され、2013 年 12 月のサービス提供開始から約 3 年半で累計導入社数・累計導入サイト数国内第1位※1 を記録しています。

※ 攻撃遮断くんの名称、ロゴは、日本国における株式会社サイバーセキュリティクラウドの登録商標または商標です。
※1 出典:「クラウド型 WAF サービス」に関する市場調査(2017 年 8 月 25 日現在)＜ESP 総研調べ＞(2017 年 8 月調査)

■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 大野 暉
設 立 ： 2010 年(平成 22 年)8 月
U R L ： https://www.cscloud.co.jp/

「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」この理念を掲げ、サイバーセキュリティクラウドでは、自社で一貫して Web セキュリティサービスの開発・運用・保守・販売を行っています。
これまで技術者が必須であった Web セキュリティの領域において、いち早くクラウド化することで「早く、簡単に、より安全」な Web セキュリティ対策を実現、運用負荷の劇的な改善を可能としたことが、高く評価されています。2018 年 10 月には業界の収益(売上高)に基づく成長率のランキン

グ、「デロイト トウシュ トーマツ リミテッド 2018 年 日本テクノロジー Fast 50」において、過去 3 決算期の収益（売上高）に基づく成長率 495.72%を記録し、10 位を受賞いたしました。これからも、全ての企業様が安心安全に利用できるサービスを開発し、情報革命の推進に貢献するために私たちは挑戦し続けます。