News Release

報道関係者各位

ニュースリリース

平成 30 年 11 月 14 日

株式会社サイバーセキュリティクラウド

【2018 年度サイバー攻撃白書　3Q レポートの攻撃分析発表】
「攻撃遮断くん」で検知した攻撃ログの約 60%が、脆弱性スキャンを目的としたアクセスであると判明
3 ヶ月で 1300 万件もの攻撃を観測

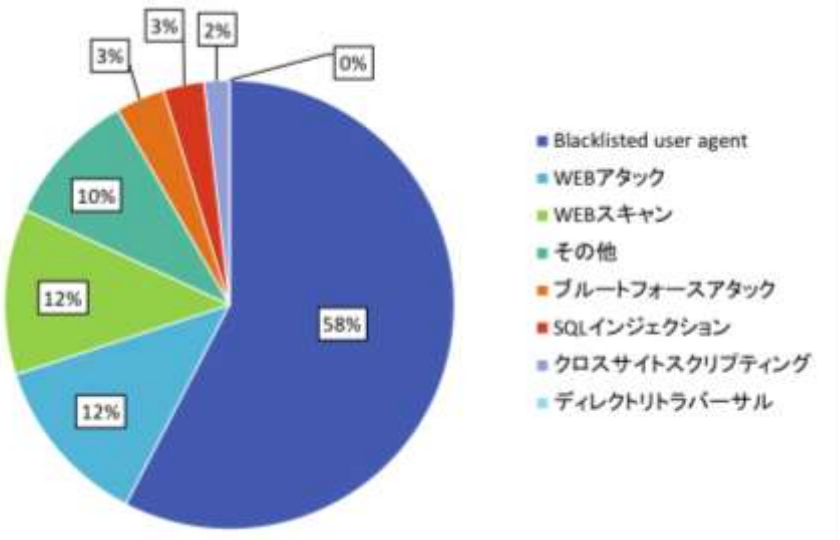
株式会社サイバーセキュリティクラウド（本社：東京都渋谷区、代表取締役：大野　暉、以下「サイバーセキュリティクラウド」）は、2018 年のサイバー攻撃の実情についてまとめた、「2018 年度　サイバー攻撃白書～3QVer.～」を発表いたします。
「2018 年度　サイバー攻撃白書」とは、Web サイトへのサイバー攻撃を可視化・遮断するクラウド型 WAF の「攻撃遮断くん」で観測した攻撃ログを集約し、分析・算出した調査レポートです。
本レポートを公開していくことで、各業界の企業に対してサイバーセキュリティに関する意識喚起を行ってまいります。

■「2018 年度　サイバー攻撃白書」概要

-調査対象期間　　:2018 年 7 月 1 日（日）～2018 年 9 月 30 日（日）
-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 3Q（7 月～9 月）での攻撃状況

2018 年 3Q（7 月～9 月）

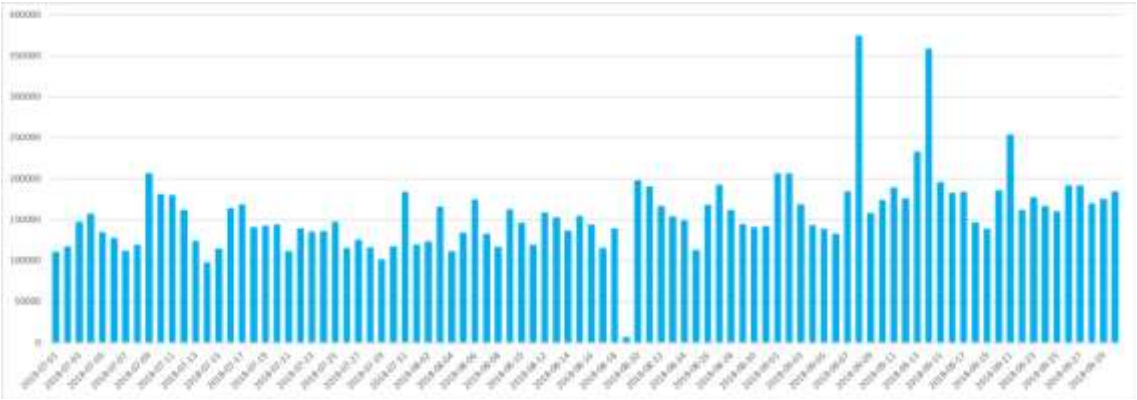


2018 年 3Q（7 月～9 月）の導入企業への攻撃状況は、「Blacklisted user agent」の攻撃が多く確認され、全体の約 60%の割合を占めており、3 ヶ月で 13,098,070 件が検知されています。
また、無作為に既知の脆弱性を試行する「WEB アタック」や、攻撃可能な Web ページを探す「Web スキャン」も昨年に引き続き多い状況となります。
併せて、2018 年 9 月には、3Q を通して最高攻撃数となる 8,668,717 件を記録しています。

■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。
以下のグラフは 2018 年 3Q 中に検知された「Blacklisted user agent」による攻撃の検知を日別でグラフ化したものです。クラウド型 WAF「攻撃遮断くん」では、一日あたり 100,000～150,000 件前後の攻撃が検知されており、最も高い数値で 374,300 件という数字が検知されています。
「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。

日別の「Blacklisted user agent」検知

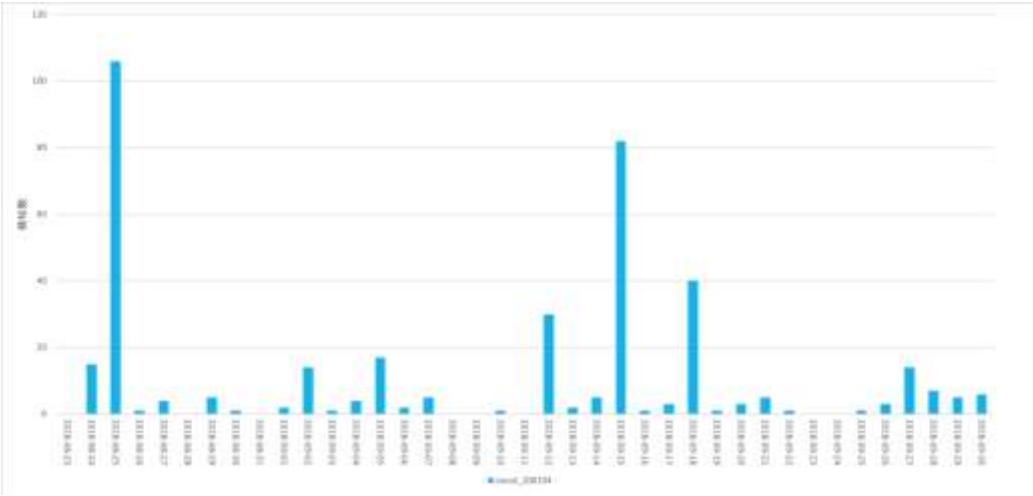


■Apache Struts2 の脆弱性について

Apache Software Foundation から 2018 年 8 月 22 日に Apache Struts2 の脆弱性（CVE-2018-11776）が発表されました。クラウド型 WAF「攻撃遮断くん」はこの脆弱性に対する攻撃を既存のシグネチャで検知できる状況ではありましたが、精度向上のために専用のシグネチャも作成し、アップデートを実施しております。下記グラフは、専用シグネチャを適用してから計測された検知ログです。8 月 24 日以降検知数が大幅に高まり、その後も攻撃が検知されていることがわかります。

脆弱性が発表された直後だけでなく、一定期間経過後も注意が必要なことがわかります。

3Q での Apache Struts2 脆弱性（CVE-2018-11776）への攻撃検知



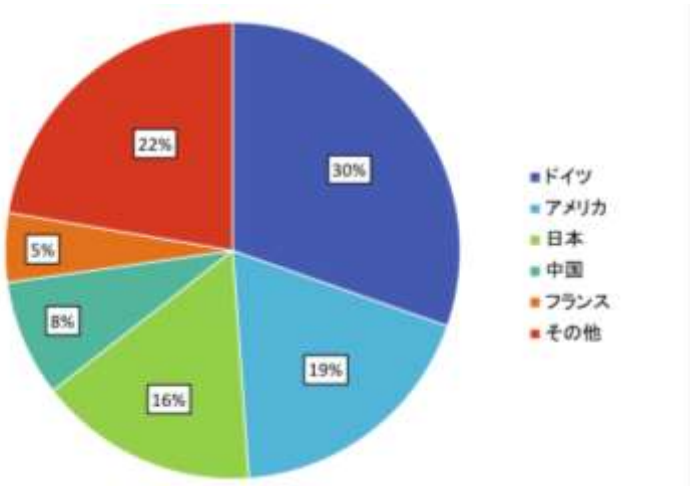
■国別での攻撃状況

2018 年 3Q（7 月～9 月）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（30%）、2 位：アメリカ（19%）、3 位：日本（16%）、4 位：中国（8%）、5 位：フランス（5%）となっております。

国別での攻撃状況

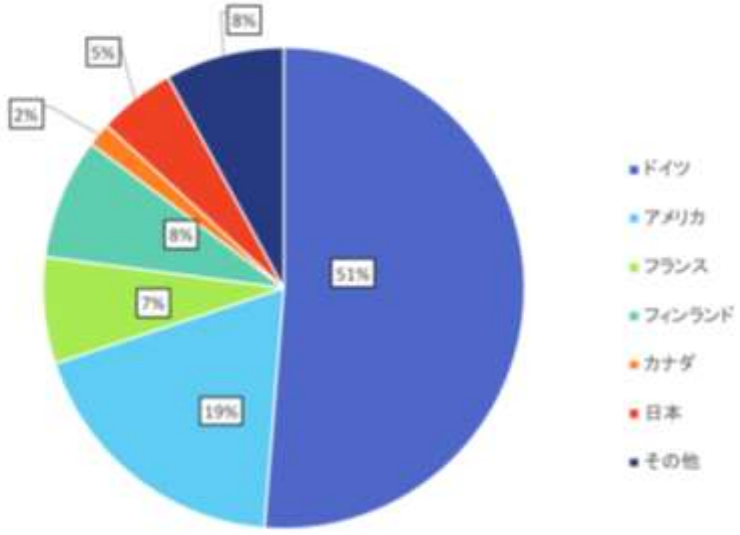


下記は 3Q での国別の「Blacklisted user agent」による攻撃検知を見た場合のグラフです。

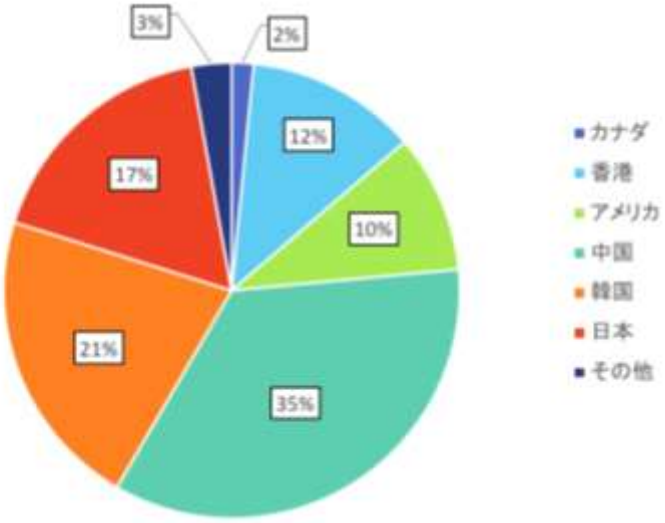
5つの国のなかでも3ヶ月を通してドイツから突出して攻撃があることがわかります。

8 月 23 日の「Apache Sturts2 脆弱性（CVE-2018-11776）」発表後の攻撃元 IP を国別で集計したグラフでは、中国からの攻撃が最も多く来ていていることが読み取れます。

3Q の国別の「Blacklisted user agent」攻撃検知



3Q での国別の「Apache Struts2 脆弱性（CVE-2018-11776）」への攻撃検知



「ApacheStruts2 脆弱性（CVE-2018-11776）」を狙った攻撃は、中国からが最も多い状態ではありましたが、「Blacklisted user agent」による攻撃はドイツが最も多く、攻撃検知を全体で見た場合にもドイツが１位であることがわかります。

■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 アタック

WEB アタックは Dos 攻撃に近い攻撃や OS コマンドインジェクションを行う攻撃です。

3.WEB スキャン

WEB スキャンは攻撃の対象を探索する動作や、無作為に行われる単純な攻撃で脆弱性を探す攻撃予兆です。

4.ブルートフォースアタック

ブルートフォースアタックは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ものです。

5.SQL インジェクション

SQL インジェクションは 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.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は攻撃者が作成したスクリプトを脆弱性のある WEB サイトを利用し閲覧者に実行させる攻撃です。

7.ディレクトリトラバーサル

ディレクトリトラバーサルは WEB サーバ上のファイルに不正アクセスする攻撃です。

8.その他

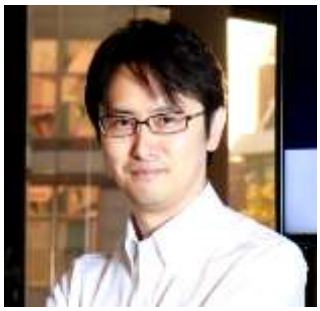
各種 OS やミドルウェアなどの脆弱性を突いた攻撃をその他としております。

通常、WAF の範囲外とされるものなども含みます。

Web サイトないし Web アプリケーションを経由しない攻撃です。

■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 8 月 23 日に Apache Struts2 の脆弱性（S02-057/CVE-2018-11776）が公開され、Apache Struts2 のバージョンを最新のものへアップデートすることが推奨されています。攻撃コード情報サイトでは、PHP に関係する脆弱性が引き続き多く報告され、HTTP/HTTPS への攻撃もその他の通信に比較して多く発生しております。

こういった Struts や PHP で開発されている Web アプリケーションの脆弱性を狙う攻撃は多く存在し、大きな被害に繋がることが予想されます。この 4 半期では、インターネットにオープンになっている Web アプリケーションに脆弱性が存在しないかスキャンする行為がクラウド型 WAF「攻撃遮断くん」でも最も多く検知されています。個人情報を持たない Web サイトであったとしても、知らない間に乗っ取られ潜伏し、攻撃のタイミングで踏み台として利用されてしまうといったリスクも考えられます。また、単なるスキャンなら防御しなくても安心というわけではありません、重要な情報が簡単に露出してしまう場合も十分あり得るスキャン内容となっています。利用しているシステムを最新のバージョンにアップデートすることも重要であり、万が一のことも考え WAF をはじめとしたセキュリティ対策の実施を検討することが必要です。

■「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。