【ニュースリリース】

2020 年 7 月 22 日

報道関係者各位

サイバーセキュリティクラウド、2020 年度上半期攻撃検知レポートを発表
～緊急事態宣言発出前と比較して宣言中はサイバー攻撃が約 20%増加～

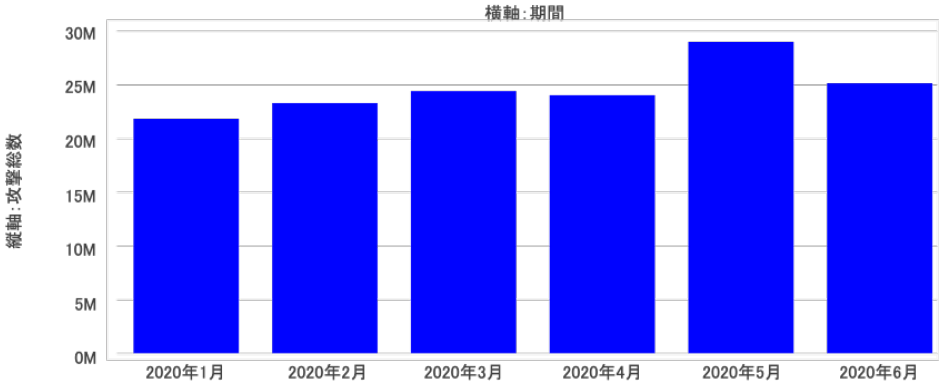
株式会社サイバーセキュリティクラウド（本社：東京都渋谷区、代表取締役社長：大野　暉、以下「当社」）は、2020 年度上半期（2020 年 1 月 1 日～6 月 30 日）を対象としたサイバー攻撃検知レポートを発表いたします。なお、本データは当社が提供する、Web サイトへのサイバー攻撃を可視化・遮断するクラウド型 WAF の「攻撃遮断くん」、AWS WAF 自動運用サービス「WafCharm（ワフチャーム）」で観測した攻撃ログを集約し、分析・算出しています。

■調査概要

・調査対象期間：2020 年 1 月 1 日～2020 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ーアカウント
・調査方法：「攻撃遮断くん」、「WafCharm」で観測した攻撃ログの分析

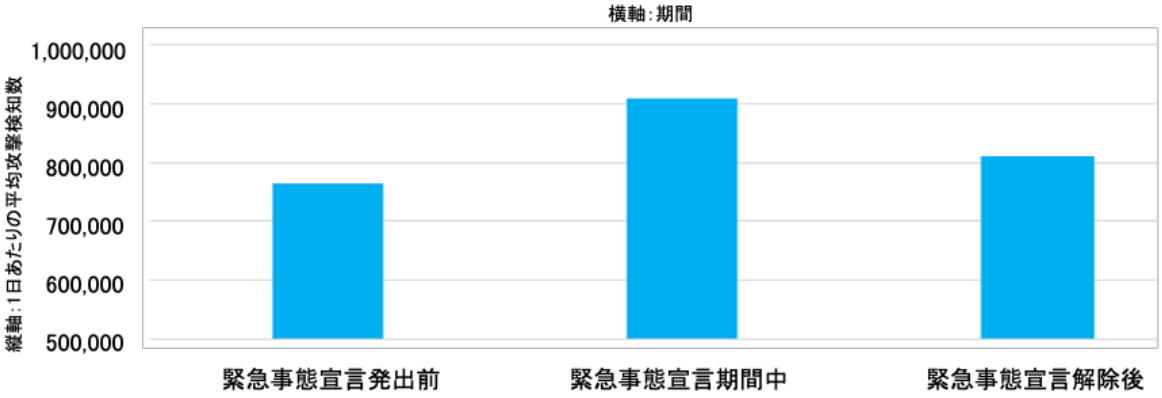
■攻撃状況

＜攻撃総数＞



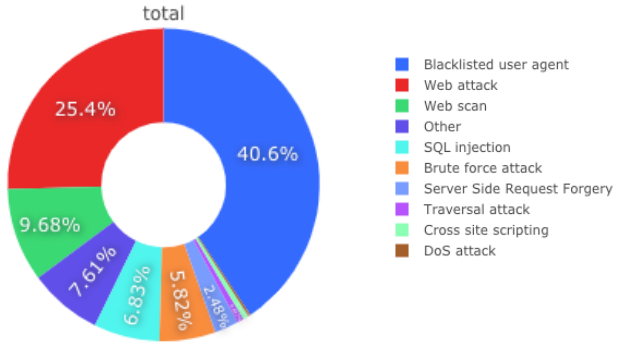
今回の調査期間における「攻撃遮断くん」、「WafCharm」を導入しているサイトにおいて検知したサイバー攻撃の総数は 147,762,255 件にのぼりました。中でも 5 月が最も多く、29,039,856 件の攻撃を検知しました。

＜緊急事態宣言発出前後の 1 日あたりの攻撃数＞



さらに緊急事態宣言発出の前後において、1 日あたりの平均攻撃数を比較したところ、4 月 7 日～5 月 25 日の緊急事態宣言期間中では、宣言発出前と比べ 19%以上多い 909,158 件の攻撃を検知しました。また緊急事態宣言の解除後、攻撃数は減少したものの、宣言発出前と比べると 6%程度増加しました。

＜攻撃種別＞



今回の調査期間において、主な攻撃種別 10 種の攻撃状況では、脆弱性スキャンツールを利用した Bot による攻撃である「Blacklisted user agent」が 59,979,416 件と全体の 40.6%を占め、次いで Web サーバー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 37,587,944 件で 25.4%、攻撃の対象を探索・調査したり、無作為に行われる単純な攻撃で脆弱性を探す方法である「Web scan」が 14,300,917 件で 9.7%を占めました。前年同時期の各攻撃種別の件数と比較すると、「Blacklisted user agent」は 1.5 倍、「Web scan」は 1.1 倍程度の増加率であったことに対して、「Web attack」は 3 倍以上増加しました。

さらに、2020 年 1 月 1 日～31 日において「Web attack」が攻撃全体に占める割合は 18.9%程度であったのに対し、5 月 1 日～30 日の間では 29.8%にまで増加しており、新型コロナの感染拡大とともに、「Web attack」の脅威が高まりました。

※Blacklisted user agent について
「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、「ZmEu」「Nikto」「Morfeus」などといったスキャンツールが該当します。

※Web attack について
「Web attack」とは Web サーバーを構成するソフトウェアの脆弱性に対する攻撃を検知したものです。

■サイバーセキュリティクラウド　取締役 CTO　渡辺洋司のコメント

2020 年上半期を振り返ると、2020 年 1 月にアメリカの Microsoft 社の「Internet Explorer」がゼロデイ攻撃を受けたことを発表し話題となりました。ゼロデイ攻撃とは修正策が存在しない脆弱性を突く攻撃で、そのため検知するのが非常に困難な攻撃でもあります。だからこそ大手企業である Microsoft 社が提供する「Internet Explorer」ですらも被害に遭ってしまいました。このようにサイバー攻撃は常に巧妙化していて、企業も常に対策をアップデートしていく必要があるでしょう。

今回の調査では、新型コロナの影響による緊急事態宣言が発出された期間にサイバー攻撃が増加し、中でも「Web attack」が急増しました。緊急事態宣言が発出された期間内では、企業にテレワーク導入が進んだことや、ゴールデンウィークがあったことことから攻撃が増加した可能性が高いと考えられます。

今後夏休みなど長期休暇を控え、再び新型コロナの感染拡大が懸念される中では、こうした攻撃への対策強化が一層重要であると考えられます。

このようにサイバー攻撃の目的や手口は多様化し、常に攻撃のタイミングを窺っています。企業規模に関わらず Web サイトを保有する組織にとって、こうしたサイバー攻撃への対策の重要性は高まっていると言えます。

【クラウド型 WAF「攻撃遮断くん」について】

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

クラウド型 WAF「攻撃遮断くん」は、Web サイト・Web サーバへのサイバー攻撃を可視化・遮断する Web セキュリティサービスです。ディープラーニング（深層学習）を用いた攻撃検知 AI エンジン「Cyneural」を活用し、一般的な攻撃の検知はもちろん、未知の攻撃の発見、誤検知の発見を高速に行うとともに、世界有数の脅威インテリジェンスチーム「Cyhorus」により、最新の脅威にもいち早く対応します。導入社数・サイト数で国内 1 位※1 を獲得し、企業規模を問わずご利用いただいています。

【AWS WAF 自動運用サービス「WafCharm（ワフチャーム）」について】

https://www.wafcharm.com/

「WafCharm」は導入ユーザ数で国内 1 位※2 の AI による「AWS WAF」のルール（シグネチャ）自動運用サービスです。機械学習を用いて最適な WAF ルールを自動運用する AI エンジン「WRAO（ラオ）※3」（特許番号：特許第 6375047 号）を搭載しています。累計導入サイト数・導入社数国内 No.1※1 の実績を持つクラウド型 WAF「攻撃遮断くん」で培った 1 兆件を超えるビックデータを活用し、お客様毎に最適なルールを AWS WAF に自動で適用します。サイバー脅威情報監視チーム「Cyhorus」により最新の脅威にもいち早く対応します。また、国内有数のシグネチャカスタマイズのノウハウをもった、開発エンジニアによるサポートも合わせて提供しています。190 か国 100 万以上の AWS ユーザーに向けて販売しています。

【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 東京都渋谷区東 3-9-19 VORT 恵比寿 maxim3 階

代表者：代表取締役社長 大野 暉

設立 ：2010 年 8 月

URL ：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」という理念を掲げ、サイバーセキュリティクラウドでは、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を全世界に向

けてサブスクリプションで提供しています。また、クラウド市場世界シェア 47.8%※4 を持つ AWS において、世界で 7 社目となる AWS WAF マネージドルールセラーにも認定されております。
これからも私たちは、リーディングカンパニーとして、世界中の人々が安心安全に利用できるサイバー空間を創造するためのサービス開発を行い、情報革命の推進に貢献してまいります。

※1 出典:「クラウド型WAFサービス」に関する市場調査(2019年6月16日現在)<ESP総研 調べ>(2019年5月～2019年6月 調査)
※2 日本マーケティングリサーチ機構調べ 調査概要:2020年7月期_実績調査
※3 AWS WAF classic のみに対応
※4 出典:Gartner(July 2019)・・・Worldwide Iaas Public Cloud Services Market Share, 2017-2018
(Millions of U.S. Dollars)

<本件のお問い合わせ>

■サービスに関するお問い合わせ先
株式会社サイバーセキュリティクラウド
マーケティング部 PR・マーケティングチーム
電話:03-6416-9996 FAX:03-6416-9997
E-mail:pr@cscloud.co.jp

■報道関係お問い合わせ先
サイバーセキュリティクラウド PR事務局(スキュー内)
担当:西尾・北出
TEL:03-6450-5457 Mail:csc@skewinc.co.jp