CDNetworks

State of the Web Security H1 2021

Phone: +65 6908 1198 Email: info@cdnetworks.com

Table of Content

Email: info@cdnetworks.com www.cdnetworks.co.jp

概要

CDNetworksが収集した攻撃分析データをご利用いただいている多くの企業や政府機関またonline service事業者などのお客様に年間セキュリティレポートとして提供しています。このレポートは様々な重要指標をあらゆる視点から分析しています。

このレポートのデータは「クラウド・セキュリティ」によって提供されています。クラウド・セキュリティ」は継続的に最適化、進化させています。

これにより攻撃と防御の状況の広範な理解を得ることができます。
レポートでは、2019年、2020年、および2021年前半の攻撃と防御のデータを包括的に比較して、攻撃の傾向などの状況を報告しています。

DDoS攻撃概要

- 2021年上半期「CDNetworks security platform」は3000万件のDDoS attackを検出しました。2020年同時期と比較し、DDoS attackのピークはわずかながらに増加しました。
- 2021年上半期の DDoS attack の数は最大となりました。従来の通り最も攻撃を受けたのはゲーム業界がトップです。
- リフレクション増幅攻撃に関しては、NTPプロトコル攻撃が急増し、攻撃の87.55%を占めました。

Webアプリケーション攻撃概要

2021年上半期、クラウド・セキュリティ」は101.13億のWebアプリケーション攻撃を監視およびブロックしました。これは2020年上半期の2.39倍、2019年上半期の21.66倍であり、Webアプリケーション攻撃が圧倒的に増加していることを示しています。

注目点としては、Webアプリケーション攻撃の標的は、政府関連からソフトウェア情報サービス、不動産、金融などの他の業界にシフトしています。

Bot攻撃概要

2021年上半期、「CDNetworks security platform」は、341億4700万のボット攻撃を監視およびブロックしました。これは、1秒あたり平均2183.52回の攻撃を受け、前年と比べ2倍になります。
ソフトウェア情報サービスは、悪意のあるボット攻撃の影響を最も受けている業界であり、不動産、運輸業、eコマースがそれに続きます。

Email: info@cdnetworks.com www.cdnetworks.co.jp

2021年上半期API攻撃の概要及びトレンド

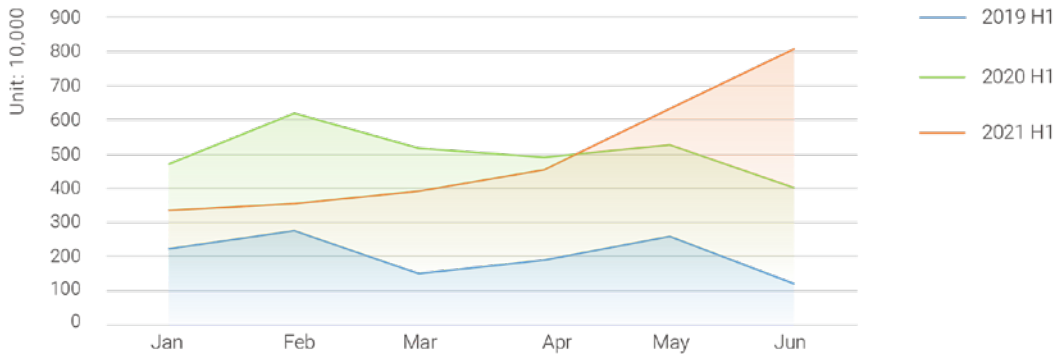
API Attack概要及び2021年上半期のトレンド
2021年上半期に「CDNetworks security platform」はAPIサービスに対する42億5300万の攻撃を監視およびブロックし、これは2020年の2倍に該当し、この攻撃タイプが大幅に増加したことを示しています。

APIへの攻撃は多様化の傾向にあります。
API攻撃のほとんどは、ソフトウェア情報サービスと金融業界に集中しており、それぞれ41.62%と28.41%を占めています。

DDoS Attacks

2021年上半期も引き続きDDoS Attackは増加傾向です。

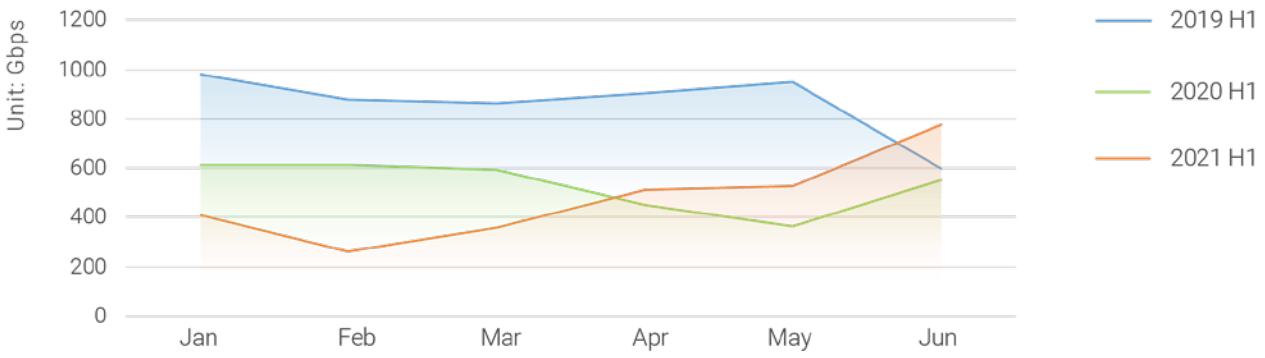
2021年上半期、「CDNetworks security platform」は、2020年と同様のDDoS攻撃を検出し、1.63%少ないだけでした。月ごとの攻撃の数は2021年前半に持続的な増加を示し、5月と6月に大幅な増加となりました。



DDoS Attack Event Trend of H1 2019/2020/2021

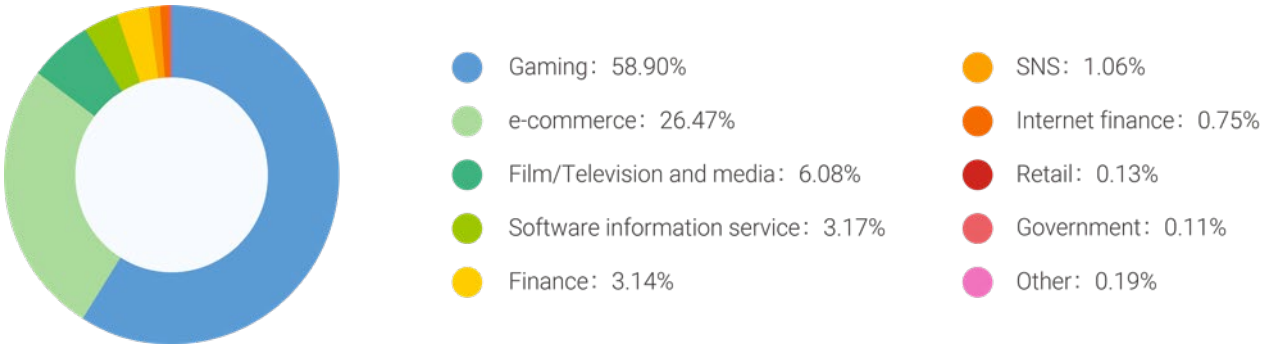
2021年上半期のDDoS攻撃のピークは6月で、774.58Gbpsに達しました。これは、2020年前半の611.73Gpbsのピークより26.62%高く、2019年前半の982.47Gpbsよりも低い値です。今年のピークも前年とは異なる月に発生し、2019年と2020年とも前半に攻撃のピークを迎えましたが、今年の月次攻撃のピークは2月に始まり、6月にピークに達しました。

Email: info@cdnetworks.com www.cdnetworks.co.jp



Monthly Distribution of DDoS Attack of H1 2019/2020/2021

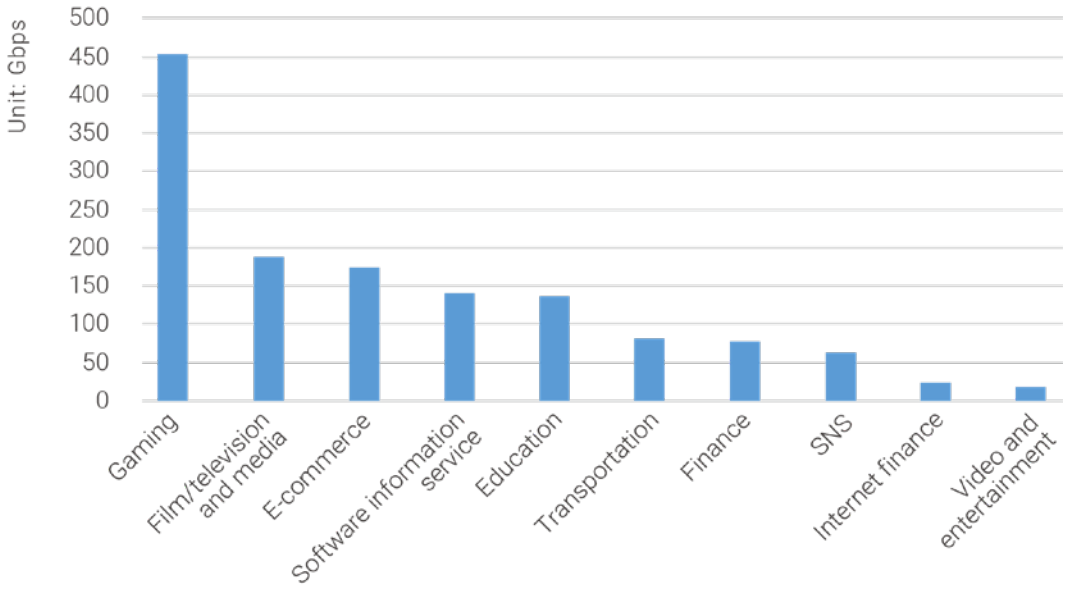
DDoS攻撃の80%以上は、ゲーム業界とeコマース業界に集中しています。



Industry Distribution of DDoS Attack of H1 2021

DDoS攻撃の業界分布に関しては、ゲーム業界は2021年上半期に最も多くのDDoS攻撃を受け、58.90%を占め、他のすべての業界を上回りました。Eコマースは26.47%で2位。両方の業界を合わせて、攻撃の85%に達しました。3位と4位は、映画/テレビとメディア情報（6.08%）およびソフトウェア情報サービス（3.17%）となりました。

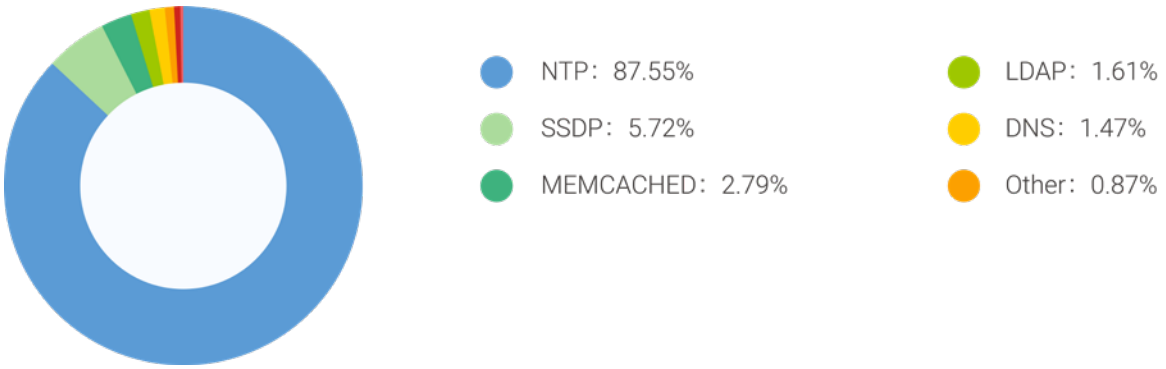
Email: info@cdnetworks.com www.cdnetworks.co.jp



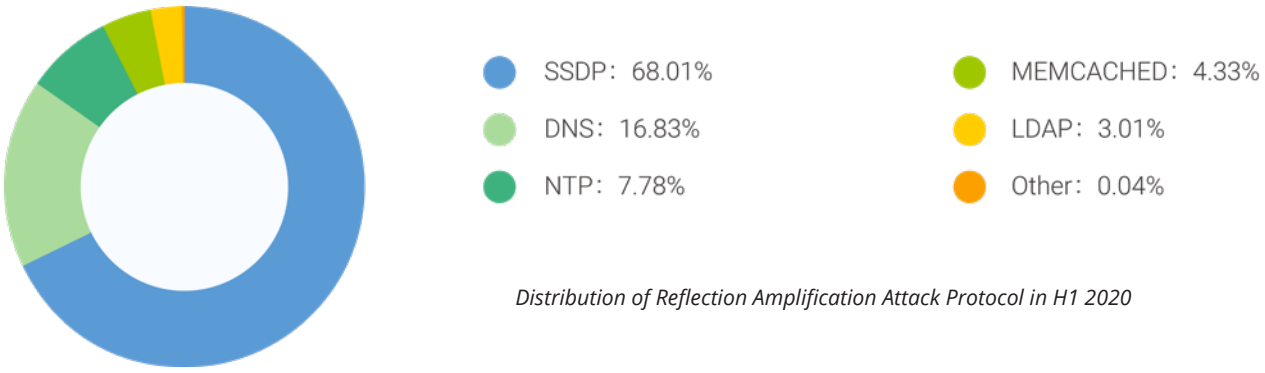
Top 10 Industries of DDoS Attack Peaks for H1 2021

さまざまな業界が受けた攻撃のピークについての統計では、ゲーム、映画/テレビ、メディア情報、eコマース、ソフトウェア情報サービス業界が上位4業界で、ゲーム業界の攻撃ピークは450Gbpsを上回っています。攻撃の数と攻撃のピークの業界分布は、業界それぞれの傾向を示しています。

主要なNTPリフレクション増幅攻撃の傾向



Distribution of Reflection Amplification Attack Protocol in H1 2021



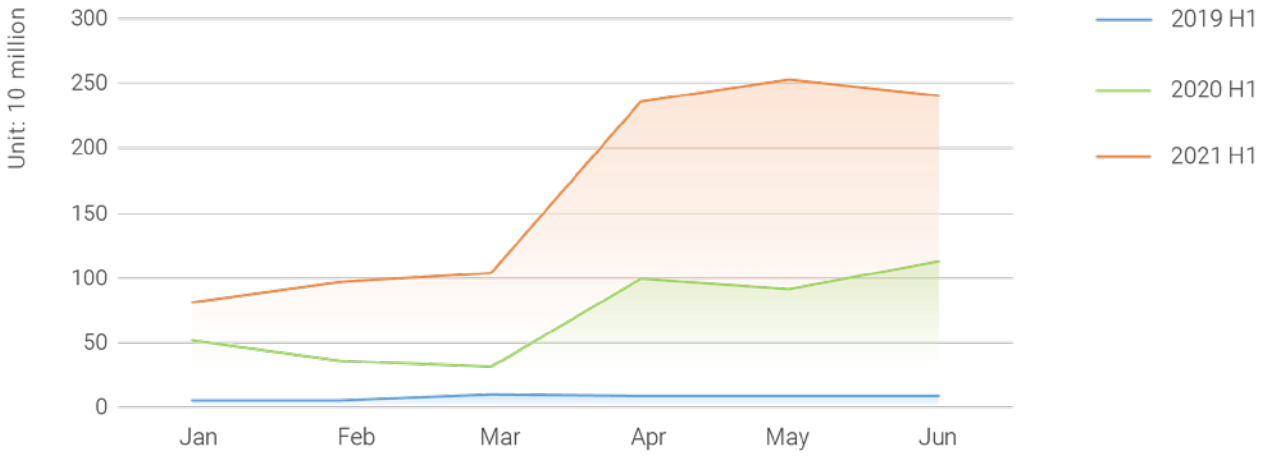
Distribution of Reflection Amplification Attack Protocol in H1 2020

NTP増幅攻撃は、最も使用されるDDoS攻撃の1つですが、2021年前半に、NTP増幅攻撃の主なプロトコルで大幅な改造が行われました。NTP増幅攻撃が発生し、これまでの主な攻撃タイプであったSSDPプロトコル攻撃を上回り、その割合は前年同期の7.78%から87.55%に急増しました。NTPプロトコルが攻撃で広く使用され、パブリックネットワーク上にまだ公開されている誤って構成されたNTPサーバーが多数残っており、ハッカーが容易に攻撃できる状況です。SSDP攻撃の割合については68.01%から5.72%に急落しました。

Web Application Attacks

2021年上半期のウェブアプリケーションアタック2020年の攻撃数を超えています。

2021年上半期に「CDNetworks security platform」は101億1,300万のWebアプリケーション攻撃を監視およびブロックし、2020年全体の攻撃数を上回りました。これは2020年と比べて139.39%増加し、倍増傾向であり攻撃の割合としては増え続けています。

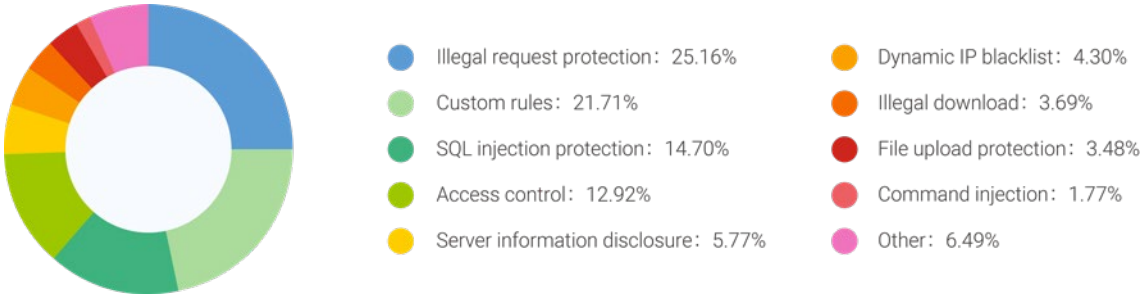


Web Attack Trend of H1 2019/2020/2021

Email: info@cdnetworks.com
www.cdnetworks.co.jp

Web attackの多様化

CDNetworksプラットフォームを搭載したWeb攻撃保護システムは、さまざまな攻撃方法に対処が出来、攻撃方法の分布を明確に確認することもできます。



Web Attack / Defense Measure Distribution of H1 2021

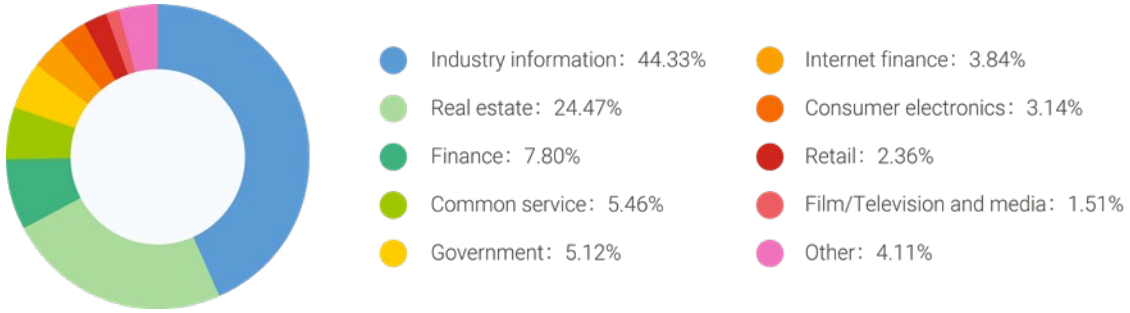
上の図からわかるように、Webアプリケーション攻撃の攻撃方法および防御的手段は、比較的均等です。上位3つは、不正攻撃（25.16%）、カスタムルール（21.71%）、およびSQLインジェクション保護（14.70%）です。また保護については前年と比較して、SQLインジェクション保護が好まれ、ブルートフォースクラッキング保護はトップ3から外れ、わずか0.53%となりました。

カスタムルールの割合が以前よりもはるかに高くなっていることは注目に値します。これは、Web攻撃保護では、ビジネス条件と特定の攻撃シナリオに基づいて特定のカスタムルールを作成することも非常に効果的であることを示しています。

自動スキャナーからのトラフィックが増加しています。「CDNetworks security platform」は、攻撃元の機能分析、動作パターン、AIモデルの検出、脅威インテリジェンスなどを通じてWebスキャナーを識別し、アクセス制御（12.92%）、動的IPブラックリスト（4.3%）でスキャナー攻撃のほとんどを直接除外が可能です。特定のWebサイトに対する標的型攻撃を効果的に低減します。同時に、ウェブサイト上の自動スキャナーの負荷圧力を減らします。

Email: info@cdnetworks.com www.cdnetworks.co.jp

ソフトウェア情報サービスへの攻撃は40億回以上に

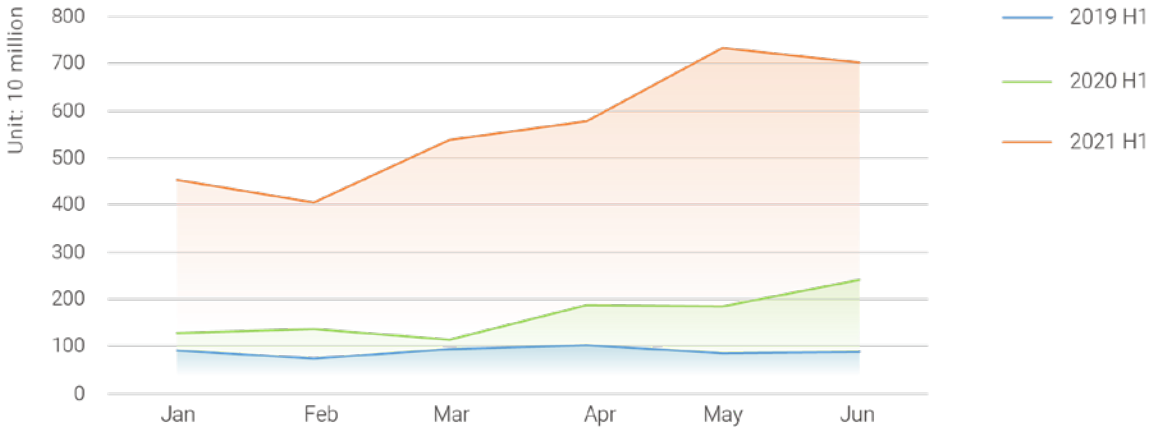


Industry Distribution of Web Application Attack in H1 2021

2021年上半期のデータによると、ソフトウェア情報サービスと不動産業界はWeb攻撃が最も多い業界で、2021年上半期のWebアプリケーション攻撃の約70%で約70億回にのぼりました。続いて金融（7.80%）、共通サービス（5.46%）、政府機関（5.12%）は、それぞれ3位から5位と続きます。

Bot Attack

悪意のあるBot攻撃は3.29倍に増加



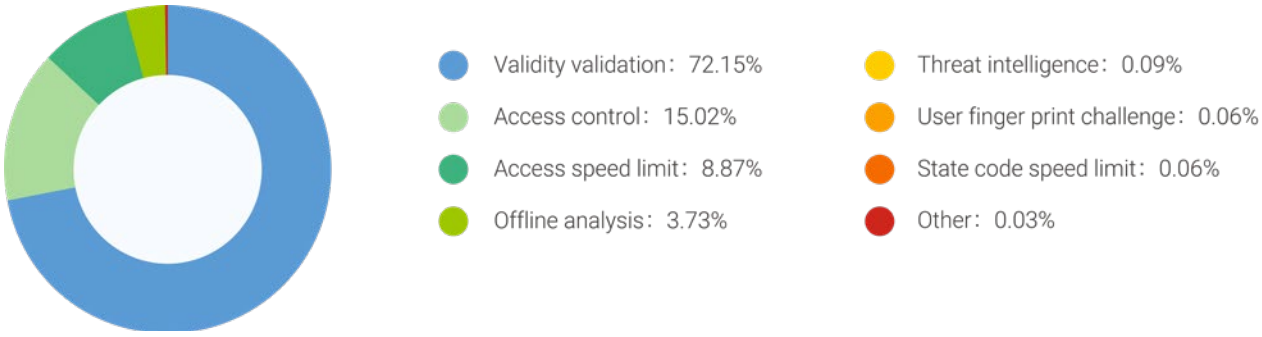
Malicious Crawler Attack Trend of H1 2019/2020/2021

2021年上半期には、「CDNetworks security platform」が341.47億回を超える悪意のあるボット攻撃を監視およびブロックし、1秒あたりの平均攻撃数は2183.52回にのぼり、2020年の合計の3.29倍でした。2019年の同時期に比べて6.34倍です。攻撃数は年々倍増しており、セキュリティの脅威はますます顕著になっています。

Email: info@cdnetworks.com www.cdnetworks.co.jp

有効性の検証で攻撃の70%以上を効果的にブロックしています

「CDNetworksプラットフォーム」は、さまざまな保護アルゴリズムと統合されて、悪意のあるボットの保護システムを確立しています。攻撃方法の傾向と防御の結果は、オンラインの攻撃と防御のデータから評価できます。

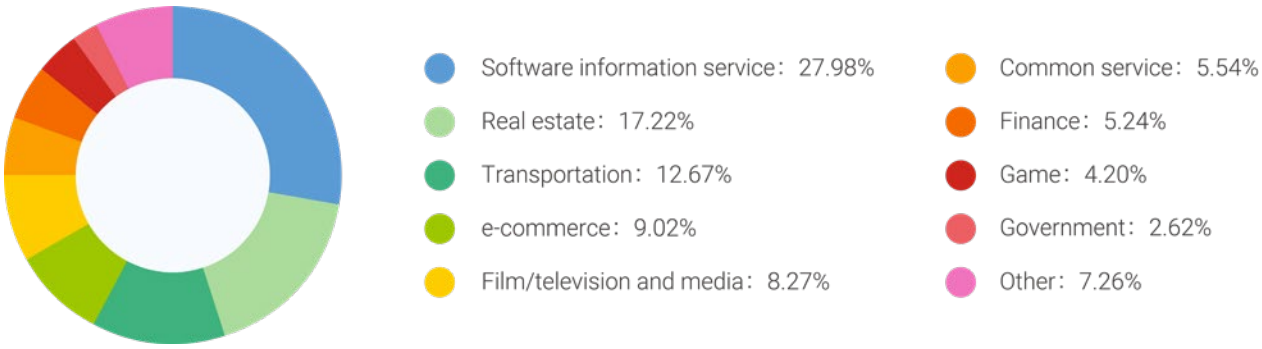


Malicious Crawler Attack / Defense Measure Distribution of H1 2021

2021年前半の攻撃と防御のデータから、クライアントとそのリクエストの有効性検証を使用したさまざまな悪意のあるボット保護方法が、悪意のあるボットに対処するための最も効果的な手段であることがわかります。

さらに、アクセス制御（15.02%）、アクセス速度制限（8.87%）、およびその他の手段も、重要な保護機能である事を示しています。

産業界は悪意のあるBot攻撃に満ち溢れている



Industry Distribution of Malicious Crawler Attack in H1 2021

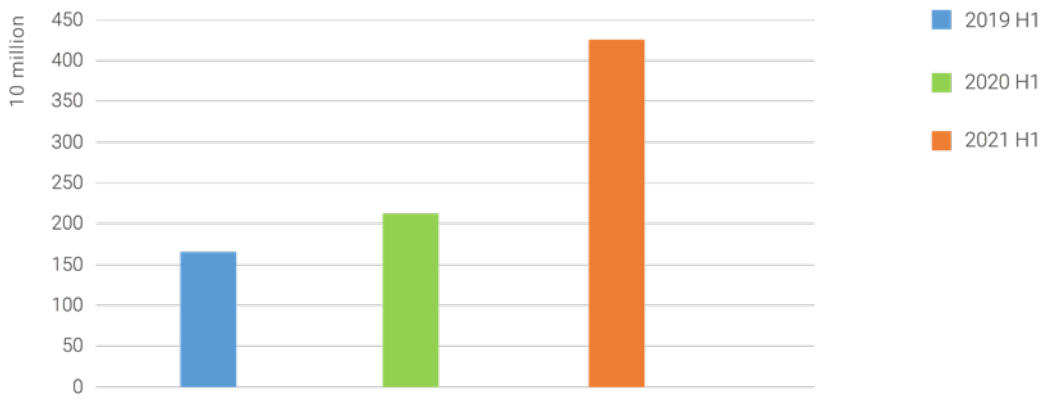
運輸業界のランキングは昨年2020年の9位（2.08%）から上位3位に上昇。
運輸業界がCOVIDのパンデミックの悪影響から徐々に回復し、航空機チケット予約ボットが復活したことを反映しています。

Email: info@cdnetworks.com www.cdnetworks.co.jp

API Attacks

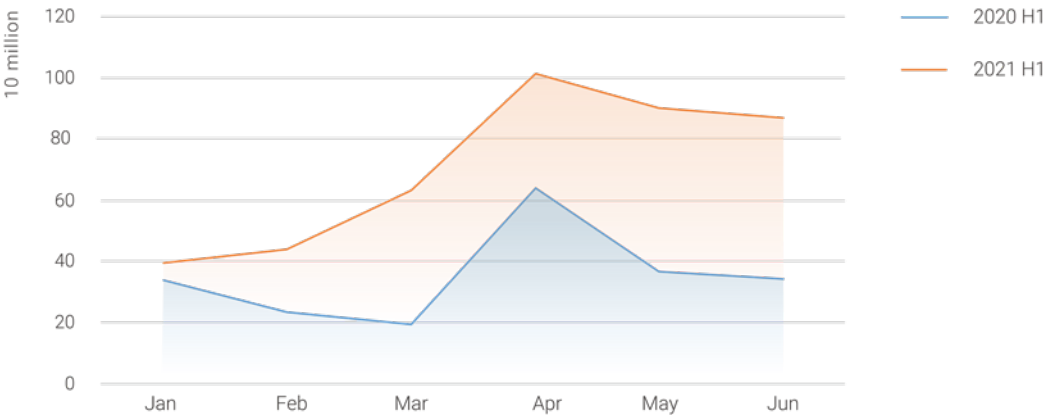
API攻撃が2.01倍と急増

インターネット、ビッグデータ、マイクロサービスアーキテクチャの利用拡大と共に、APIは大幅な成長を遂げました。オープンAPIは、さまざまなインターネット製品やサービスの開発に便利ですが、攻撃者にとっては収益性の高いターゲットとなります。



API Attacks of H1 2019/2020/2021

2021年上半期には、「CDNetworks security platform」がAPIサービスに対する合計42億5300万の攻撃を監視およびブロックし、1秒あたりの平均攻撃数は271.96回で、2020年同時期の2.01倍に達し、非常に増加しました。年々、APIサービスは深刻なセキュリティの脅威が増すとの見通しを示しています。

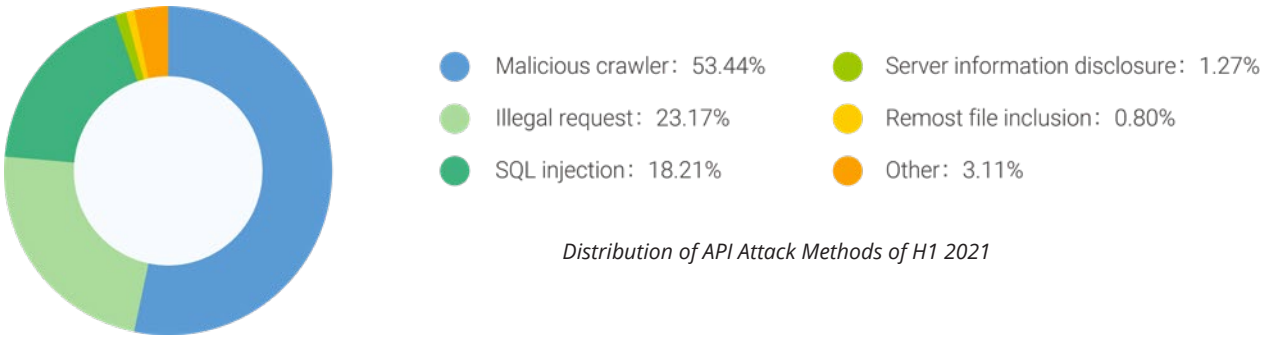


Monthly Distribution of API Business Attack in H1 2020 and H1 2021

Email: info@cdnetworks.com www.cdnetworks.co.jp

月次の傾向としては、2021年の上半期におけるAPIに対する攻撃は1月以降増加しており、4月は2020年同期とほぼ同様の増加がみられます。

API攻撃の多様化

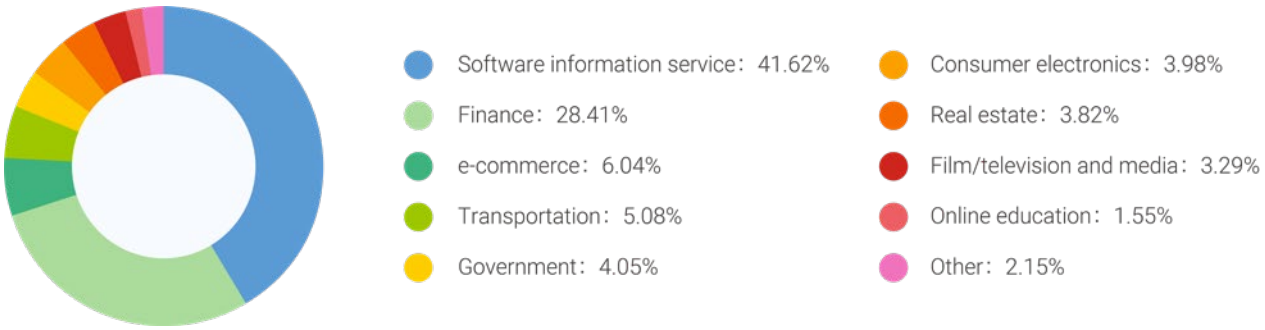


Distribution of API Attack Methods of H1 2021

APIサービスに対する攻撃では、悪意のあるボットが最も利用されている攻撃方法であり、この傾向は継続的に増加しています。2021年上半期のAPI攻撃データでは、悪意のあるボット攻撃が攻撃総数の53.44%を占め、2021年の同時期からは74.82%と大幅に減少しました。

2位と3位は違法リクエスト（23.17%）とSQLインジェクション（18.21%）で、昨年同期の5.97%と10.94%に比べて大幅に増加しました。用いられる攻撃手法は集約化が進んでいる。一方APIに対する攻撃は、1つの攻撃手法だけに頼るのではなく、様々な手法交えて用いる傾向にあることがわかります。

ソフトウェア情報サービスと金融業界は、API攻撃の最も大きな打撃を受けた分野になっています。



Industry Distribution of API Attack in H1 2021

Email: info@cdnetworks.com www.cdnetworks.co.jp

2021年上半期では、ソフトウェア情報サービス業界が最も多くのAPI攻撃に苦しんでおり、攻撃量全体の41.62%を占めています。続いて金融業界で28.41%になります。

これら2つの業界が受けるAPI攻撃の割合は合わせて70%近くに達し、この2つの業界は非常に激しい攻撃に晒されています。

過去数年間にAPI攻撃の大部分が政府機関向けであったが、今年上半期の攻撃は前年同期の約10%に急減し、2020年上半期の60.94%から4.05%に減少しました。

傾向と特徴

レポートのデータからわかるように、攻撃手法は絶えず変化しており、このセキュリティレポートに示されているデータと攻撃および防御のシナリオは、2019年と2020年の同時期と比較していくつかの変更が加えられています。また、自社のビジネスが直面するセキュリティの脅威を認識するにあたり、企業は常に適応する必要があります。

ネットワーク層のDDoS攻撃と比べ、アプリケーション層とビジネスデータに対する攻撃は増加しています。

このレポートでも触れられている通り、Web攻撃、悪意のあるボット攻撃、およびAPI攻撃はすべて指数関数的に増加しています。一方、ネットワーク層でのDDoS攻撃は鈍化する傾向にあり、アプリケーション層やビジネスデータを狙った攻撃が増加し、割合も増加しています。攻撃の目的は、単にビジネスデータにアクセスできない様にするだけでなく、ビジネス関連のデータなどを盗みとる事でもあります。攻撃者が攻撃に成功すると、ビジネス自体に影響を与えるだけでなく、漏洩したデータも悪用され侵入者の利益になります。キャプチャされたサーバーは、他のターゲットに対してマイニングまたは攻撃するためのリソースになるため、攻撃者にとってより多くの利益を生み出し、被害をうけた企業は多く、長期的に損害をもたらします。攻撃方法に関しては、ハッカー攻撃は自動化に加え発見を難しくするためにさらに巧妙化しています。AIを利用して人間の行動をシュミレーションし、従来のセキュリティポリシーをかいくぐり、侵入検知と保護がより一層困難になっています。

包括的なクラウドセキュリティソリューションが一般化するでしょう。

オンラインサービスを提供する場合、企業はネットワーク層からアプリケーション層までの包括的なセキュリティ保護ソリューションを慎重に検討して、仮にセキュリティ対策の1つの層が破られた場合、さらなる脅威を阻止し、攻撃を防ぐために複数のレイヤーに対して幅広い安全対策手段を講じる必要があります。主要なビジネスアプリケーションとデータにアクセスさせずに損失を出さない事が重要です。

Email: info@cdnetworks.com www.cdnetworks.co.jp