日本

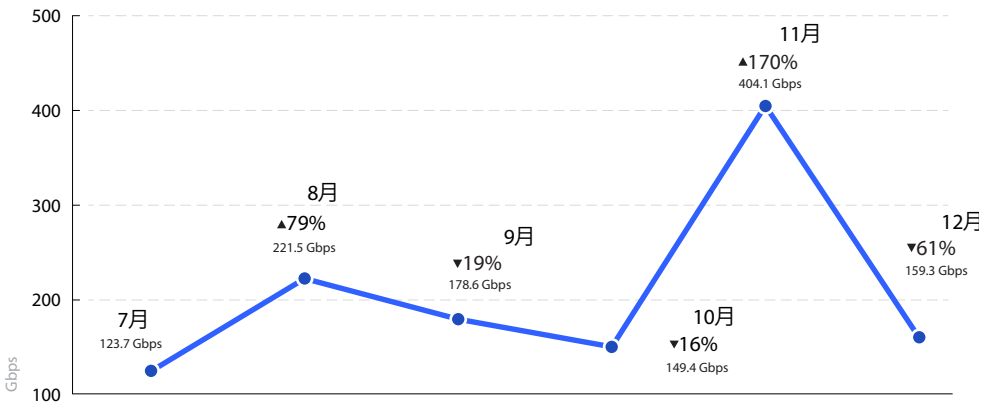
2020年下半期NETSCOUT脅威インテリジェンスレポートを基にしたキーメトリクス

COVID-19のパンデミックが引き金となり、インターネットの利用状況が大きく変化すると、サイバー犯罪者は早速、リモートワークやオンライン生活に欠かせないオンラインサービスの機能を麻痺させることを目的とした、1,000万回を超えるDDoS攻撃を仕掛けるようになりました。eコマース、ストリーミングサービス、オンライン学習、医療分野など、パンデミック下で極めて重要な産業では一様に、世界各地の何千もの企業を襲ったDDoS脅迫攻撃のLazarus Bear Armadaキャンペーンの裏で行われたものを含め、悪意をもつ攻撃者の標的となっていることが一層感じられるようになりました。COVID-19のパンデミックが2021年まで長引いていることで、攻撃者が世界的危機で明らかになった脆弱性を狙い撃ちし、さらにニューノーマル時代の弱点を突くような新たな攻撃ベクトルを見つけて利用するであろうことは論理的に推測できます。

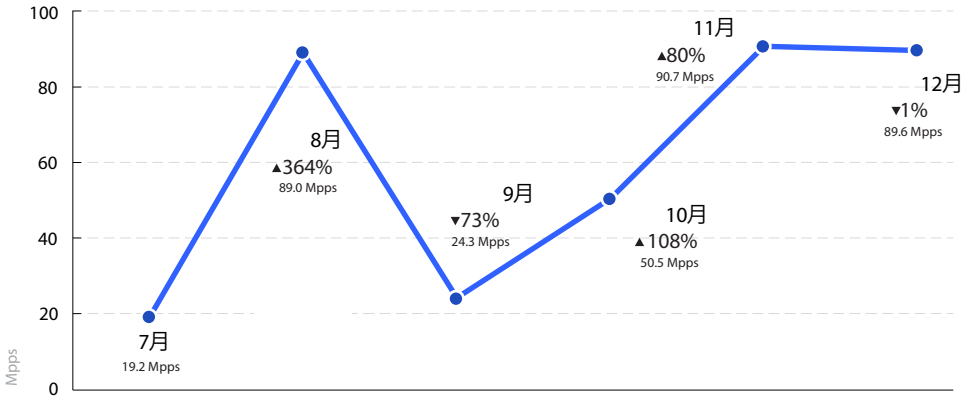
インパクト分析

DDoS攻撃の記録破りの年となったことで、グローバルインフラストラクチャは大きな影響を受けることを余儀なくされました。これは、DDoS攻撃には輸送コストがかからないためです。それどころか、一般的にそのコストはあらゆるインターネット利用者に回ってきます。そのため当社は、グローバルインターネットのどの程度のトラフィックがDDoS攻撃のみによるものかを、DDoS攻撃係数 (DAC) を計算することで、引き続き掘り下げていきました。この計算で示されたのは、DDoS攻撃がすべての地域で継続的に行われているということです。要するに、いわば「DDoS税」を私たちが支払うはめになることが示されたのです。

回線容量のインパクト率変化



処理量のインパクト率変化



DDoS統計

攻撃頻度	▲ 75%
最大処理量	▼ 91%
平均期間	▼ 14%
最大攻撃サイズ	▼ 37%

最大の攻撃

サイズ	174 GBPS
速度	34.1 MPPS
期間	12分

攻撃タイプ

NTPアンプ、CLDAPアンプ、DNSアンプ、ICMP、TCP SYN/ACKアンプ、TCP SYN、TCP ACK

ベクトル攻撃

1回の攻撃で確認されるベクトルの最大数 **19**

ベクトルトップ5	攻撃数
TCP ACK	51,459
TCP SYN/ACKアンプ	8,726
TCP RST	7,294
TCP SYN	6,304
DNSアンプ	4,320

NETSCOUT

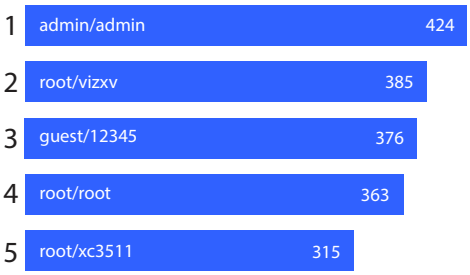
攻撃を受けたバーティカル産業トップ10

以下の産業表が示しているのは、2020年の攻撃数において最も対象となった分野です。

順位	バーティカル	頻度	最大攻撃数	最大インパクト	平均期間
1	有線通信業	4,153	116.1 Gbps	10.2 Mpps	88.9分
2	電子ショッピング + 通信販売会社	4,013	116.1 Gbps	29.8 Mpps	85.8分
3	データ処理、ホスティング + 関連サービス	3,053	107.6 Gbps	22.6 Mpps	63.3分
4	電子計算機製造	2,545	106.3 Gbps	9.3 Mpps	63.2分
5	無線通信業	2,289	116.1 Gbps	10.2 Mpps	125.9分
6	その他の通信業	1,127	116.1 Gbps	10.2 Mpps	97.3分
7	インターネット発行、配信 + Web検索ポータル	936	96.1 Gbps	8.4 Mpps	77.8分
8	コンピュータ設備管理サービス	298	49.3 Gbps	5.2 Mpps	71.7分
9	市場調査 + 世論調査	282	2.0 Gbps	0.3 Mpps	47.3分
10	電気通信販売代理店	201	96.4 Gbps	8.4 Mpps	107.3分

IoT

ユーザーネーム + パスワードの組み合わせトップ5



エクスプロイトトップ5

エクスプロイト名	EDB-ID
/picsdesc.xml Realtex SDK – Miniigd UPnP SOAP	37169
/ctrlt/DeviceUpgrade_1 HUAWEI (ファーウェイ) のルーター	45991
/setup.cgi Netgearリモートコード実行	43055
/ws/v1/cluster/apps Hadoop YARN ResourceManager	45025
/GponForm/diag_Form Dasan GPONホームルーター	-----

ビッグピクチャー

2H 2020 NETSCOUT脅威インテリジェンスレポートをすべて良くお読みいただくことで、世界的なDDoS脅威のランドスケープを通した最新のトレンドおよびアクティビティに関する研究について、ご理解いただけます。

レポートをお読みください

NETSCOUT

© 2021 NETSCOUT SYSTEMS, INC.All rights reserved.NETSCOUT、およびNETSCOUTのロゴは、合衆国および/または他国にあるNETSCOUT SYSTEMS, INC.、および/または同社の子会社、および/または関連組織の登録商標です。その他すべてのブランドおよび製品名、ならびに登録/未登録商標は、それぞれの所有者の単独所有となります。

SECR_018_JP-2101 04/2021