2021年版

企業におけるIoTの利用
誰もいないオフィスにおける脅威

職場に放置されたスマートデバイスに
起きていること

zscaler™

2020年の年初から世界的に流行した新型コロナウイルスの影響により、2021年になっても、多くの企業ではオフィスへの出勤を控えていることから、従業員の空席が目立っています。しかし、従業員が不在にもかかわらず、これらの建物の中では、水面下で活動しているものがありました。放置されていたのは、建物だけではなかったのです。スマートウォッチ、デジタルサイネージ、ネットワークプリンター、その他多くのIoTデバイスがネットワークに接続されたまま、データを更新し、その機能を実行し、コマンドを待っていたのです。

ここに脅威アクターが目を付け、多くがこの機会に乗じようとしました。今、どこからでも仕事ができるようにするべく、世界全体が大きな変革の最中にあります。結果、一時間に833ものIOTマルウェアがブロックされるという驚異的な結果となって反映されました。

スマートウォッチやIPカメラから、自動車、音楽用家具まで、IoTデバイスは企業ネットワークの中へ続々と進出しています。すべてのデバイスは、少なくとも通信の一部にSSLを使用していますが、トランザクションの76%は暗号化されていない平文で行われています。組織は、ゼロトラストポリシーとアーキテクチャを採用して、これらのデバイスを経由した悪用からネットワークを守る必要があります。ゼットスケーラーのThreatLabzチームによって作成された本レポートは、ゼットスケーラークラウドからの2週間分のデータに基づき、認可されたIoTデバイスと認可されていないIoTデバイスの両方とIoTマルウェアの傾向について分析したものです。

分析したデータは、事業所のほとんどが閉鎖されていた2020年12月15日から12月31日の間に、IoTデバイスとトラフィックを特定するIoTデバイスフィンガープリント調査と、ゼットスケーラークラウドのデータを基にしたIoTマルウェア調査から抽出・収集されました。IoTデバイス、特に非認可のデバイスには、エージェントが存在しないため、本レポートのすべてのデータは、物理的なオフィスの場所にある企業ネットワーク上のデバイスと攻撃を表しています。

主な調査結果

- → 世界の従業員の多くが自宅で仕事をしているにもかかわらず、企業ネットワーク上のIoTマルウェアは、2019年の調査と比べて700%も増加
- → エンタテインメントデバイスやホームオートメーションデバイスは、その種類の多さ、暗号化された通信の割合の少なさ、そして不審なデスティネーションとの接続などから、最もリスクが高い
- → GafgytとMirai—ボットネットでよく使われるこのマルウェアファミリーは、Zscalerクラウドでブロックされ たIoTマルウエアペイロードの97%を占めている
- → IoT攻撃の被害者の98%は、テクノロジー、製造業、小売・卸売業、および医療の各業界で占められている
- → ほとんどの攻撃は、中国、米国、およびインドに由来
- → IoT攻撃の標的のほとんどが、アイルランド、米国、および中国

IoTデバイスフィンガープリンティング

最も一般的なデバイス

ThreatLabzは、5億件以上のIoTデバイスのトランザクションを調査し、212社のメーカーの553種類のデバイス種別を特定し、21のカテゴリーに分類しました。それにより、セットトップボックス（29%）、スマートテレビ（20%）、スマートウォッチ（15%）の3つのカテゴリーが最も多く、—デバイス全体の約65%—を占めていたことがわかりました。

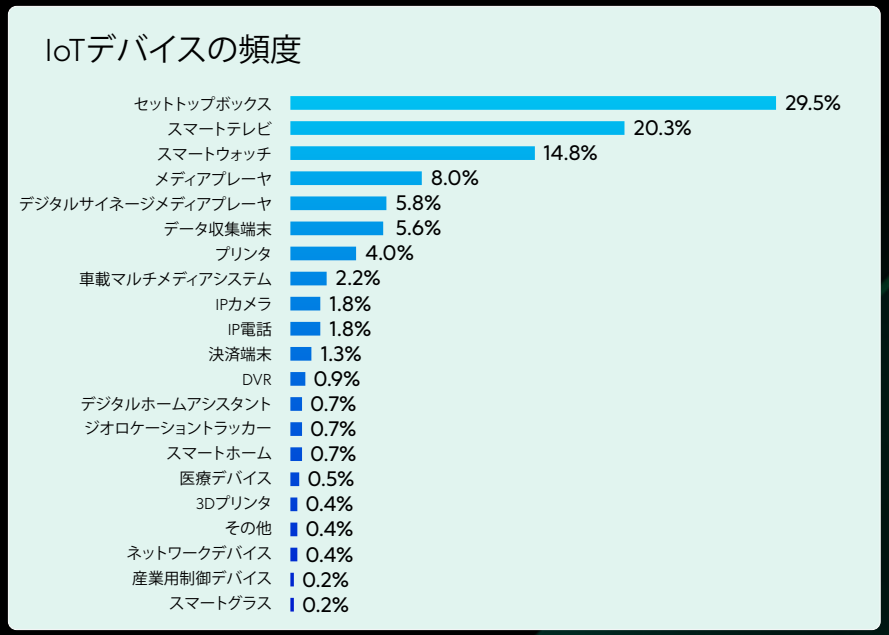
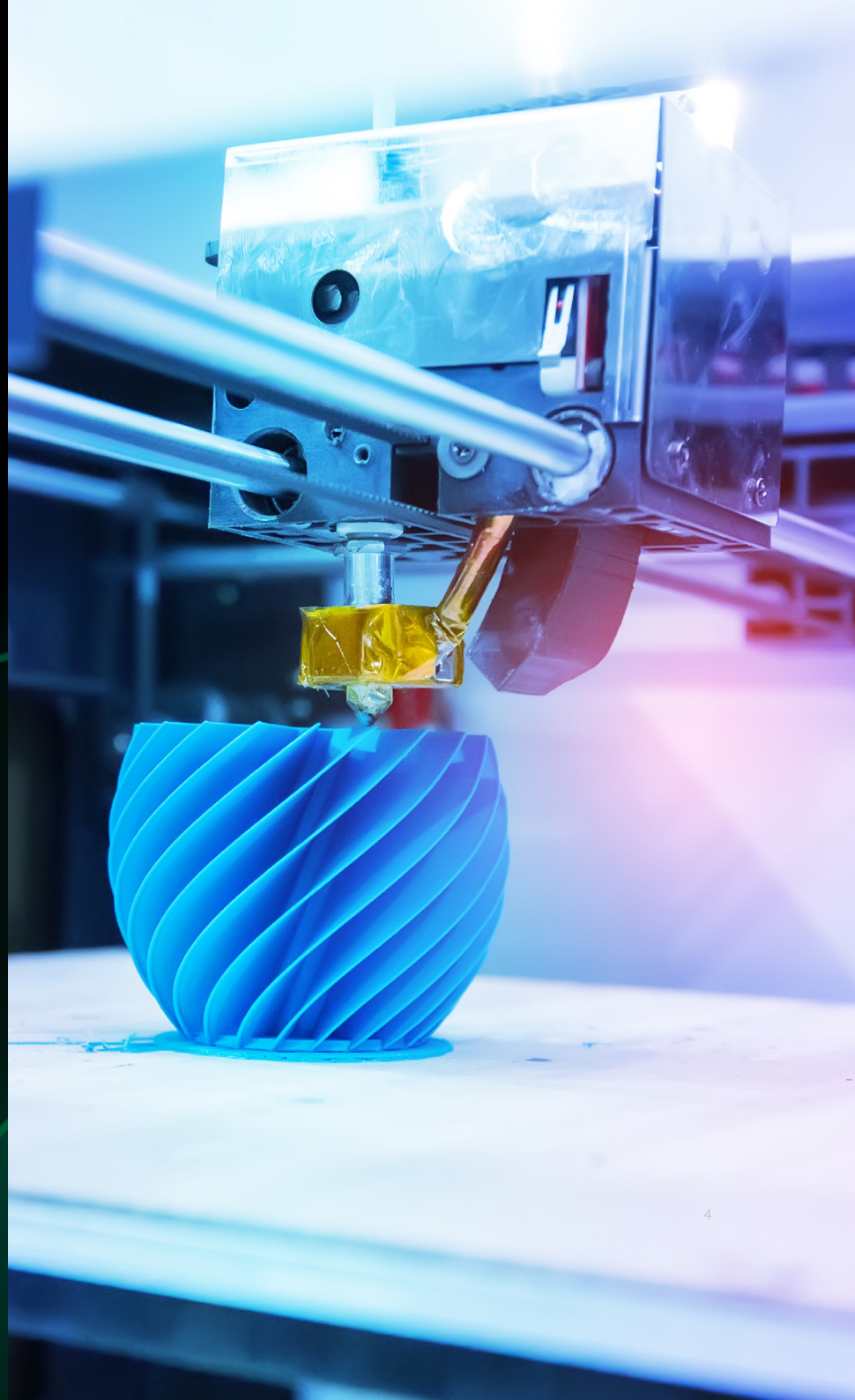


図1：IoTデバイスの頻度



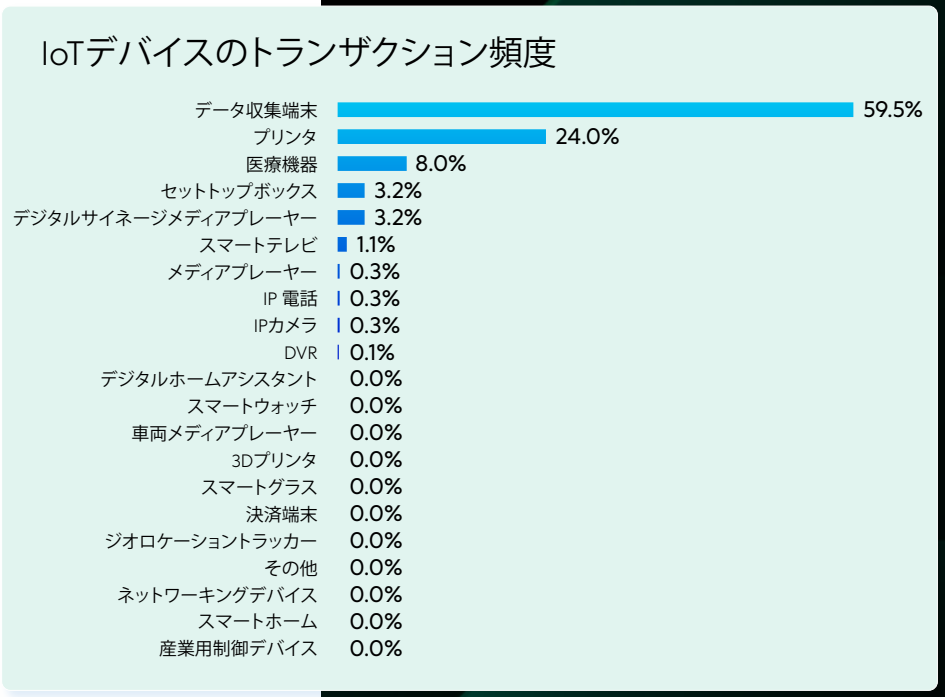
音楽用家具のインターネット？

「モノのインターネット」は新たなカテゴリーに拡大し続けていますが、その中 にはITチ ー ムが全 く目 を向 けていないものもあります。ThreatLabzは、以下のような想定外のデバイスがクラウドに接続されているのを発見しました。

- **スマート冷蔵庫：** サムスンのスマート冷蔵庫は、冷蔵庫のドアに設置されたスクリーンに、所有者の携帯電話から音楽やビデオ、コンテンツをストリーミングする機能を備えています。
- **音楽ランプ：** IkeaとSonosは、テーブルランプとスマートメディアプレーヤーを組み合わせたデバイス「Symphonisk」を開発しています。
- **自動車：** テスラとホンダの自動車用メディアプレーヤーがそれぞれ企業のネットワークに接続されているのが確認されています。
- **Wi-Fiメモリーカード：** 写真の保存や共有のためにカメラで一般的に使用されているEye FiのWi-Fiメモリーカードが、ゼットスケーラーのクラウドを介してトラフィックを送信していました。

おしゃべりなデバイス

IoTデバイスのトランザクションは、2週間の期間中、ゼットスケーラーのクラウド上の全トランザクションの0.038%を占めました。一部のデバイスは、他のデバイスよりも多くのトランザクションを占めており、図2に示すように、データ収集端末とプリンターは、それだけでIoTトラフィック全体の80%以上を占めていました。



ベース：575,091,158件のIoTデバイスからのトランザクション
図2: IoTデバイスからのトランザクション

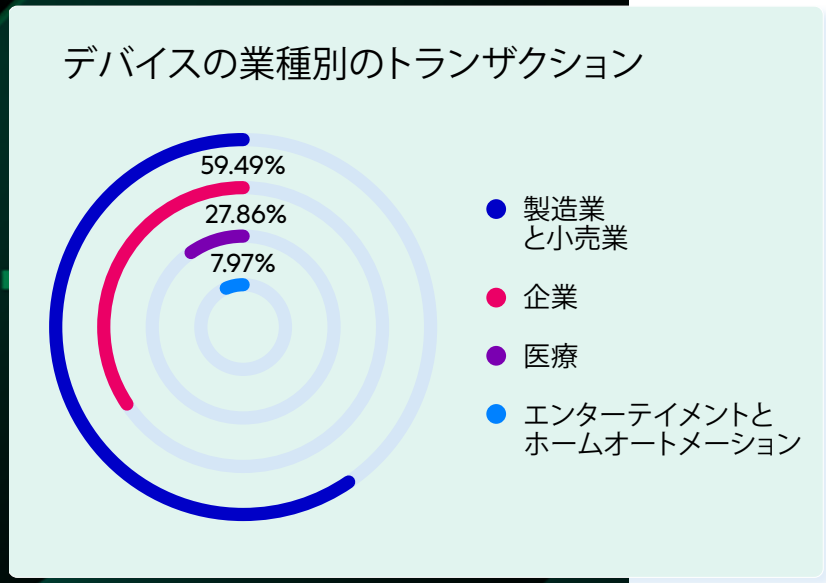


図 3: 種類別のIoTデバイス

デバイス別のトラフィック – 業種の分類

さらに、IoTデバイスは、トランザクションが発生している業界別に4つのカテゴリーに分類されました。

- **製造業 /小売業向けデバイス**
  トランザクションの59%を占めます。20社のメーカーの57種類のデバイスが含まれ、3Dプリンター、ジオロケーショントラッカー、産業用制御機器、自動車用マルチメディアシステム、データ収集端末、決済端末が含まれています。

- **企業向けデバイス**
  トランザクションの28%を占め、デジタルサイネージメディアプレーヤー、デジタルビデオレコーダー、IPカメラや電話、プリンター、ネットワーク機器が含まれています。

- **医療用デバイス**
  トランザクションの8%を占め、主にGE Healthcare、Abbott Laboratories、HOLOGICの3社の多くの医療用デバイスが含まれていました。

- **エンターテイメントとホームオートメーションデバイス**
  トランザクションの5%を占め、デジタルホームアシスタント、メディアプレーヤー、セットトップボックス、スマートグラス、スマートホーム機器、スマートテレビ、スマートウォッチなど、多種多様なデバイスからトランザクションが発生していました。これらのトランザクションの割合は最も低いものの、最も種類が多く、150社のメーカーの合計420種類の消費者デバイスが含まれています。

IoTデバイスの通信は ほとんどのケースにおいて平文

ThreatLabzは、IoTデバイスからのトランザクション全体の76%が平文のチャネルで発生しており、セキュアな暗号化チャネルで発生したトランザクションは24%に過ぎないと確認しました。この比率は受け入れがたいほど低いように見えますが、2019年の調査では、IoT通信の8.5%しか暗号化されていなかったことを考えると、ほぼ3倍に改善されています。それでもなお、セキュリティリスクは存在します。平文の通信は、攻撃者が盗み見たり、最悪の場合、傍受して変更したりすることがはるかに容易なため、IoTデバイスを悪意ある目的で利用することを許してしまいます。

今回調査した553台のデバイスすべてが何らかの形でSSLを使用していましたが、実際に暗号化された通信の割合はデバイスの種類により大きく異なりました。企業向けデバイスやホームエンターテインメントデバイスはほとんど平文で通信していたのに対し、医療用デバイスの約半分がSSLで通信していました。

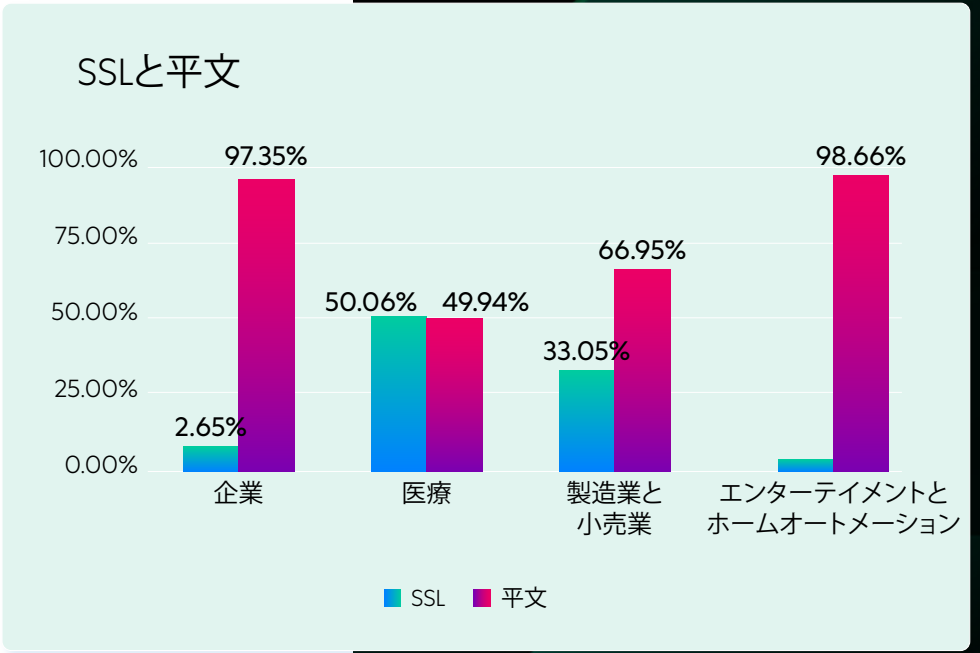


図4：デバイス種類別の暗号化通信の割合

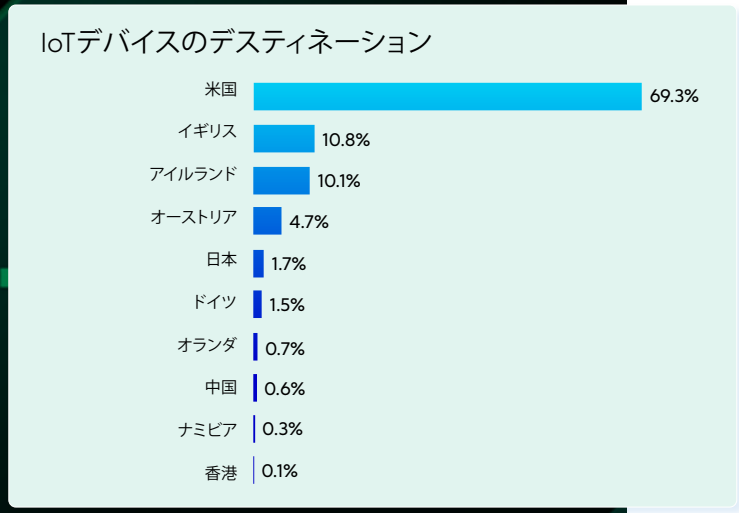


図5：IoT通信の上位デスティネーション

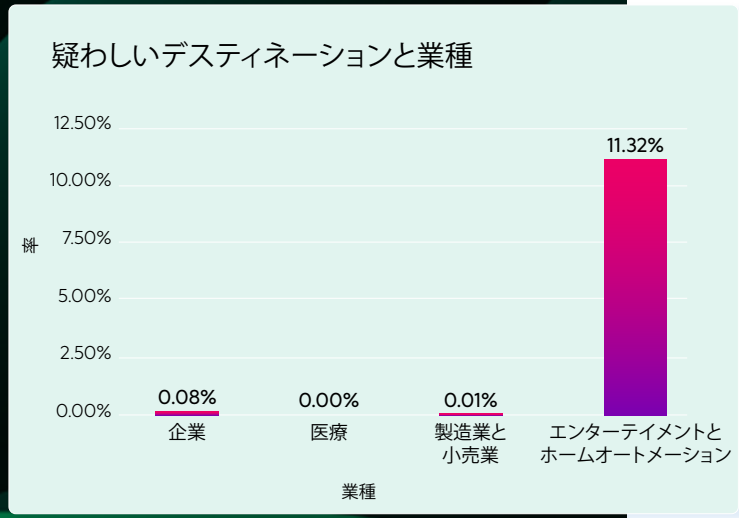


図6：デバイス種類別の不審なトラフィックの割合

IoTデバイスはどの国と会話しているのか？

ThreatLabzは、IoTデバイスがデータをルーティングしている国（「デスティネーション」）を調査しました。この通信のほとんどは合法的で、IoTデバイスはデータを送受信するという本来の役割を果たしています。デスティネーションは、米国が圧倒的に多く、トラフィックの69%を占め、イギリス (11%)、アイルランド (10%)が続きます。デスティネーションの上位10か国は以下の通りです。

エンターテイメントデバイスやホームオートメーションデバイスは、多くの場合、中国やロシアへルーティングされている

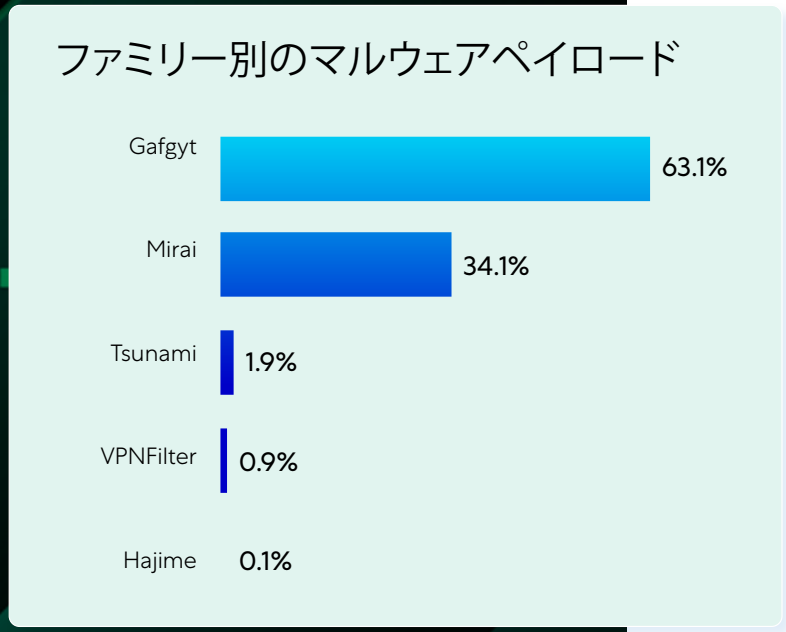
エンターテイメントデバイスとホームオートメーションデバイスからのトラフィックの11%が、中国とロシアに向けられたものでした。これらの多くは悪意のない合法的なトラフィックですが、政府のスパイ行為やその他のデータの脆弱性の可能性があるため、ThreatLabzが疑わしいと判断したデスティネーションです。この不審なトラフィックのほとんど (99.9%) は、スマートテレビやセットトップボックスからのものでした。

逆に、企業、医療、製造業や小売業向けのデバイスでは、不審なデスティネーションとの間を行き来するトラフィックの割合は0.1%未満でした。

IoTマルウェアの調査

ThreatLabzは、IoTフィンガープリント調査を行ったその2週間の間に、ゼットスケーラーのクラウド内のIoTマルウェアに特有の活動についても調査しました。

ThreatLabzは、IoTマルウェア、悪用、コマンドコントロール通信に関連して約30万件のトランザクションがブロックされたことを確認しました。これは前年比で約700％の増加となります。マルウェアのトランザクション量の中では、15日間で合計18,000のユニークホストと約900のユニークペイロードの配布が観測されました。



ベース：900 ペイロード
図7：ファミリー別のユニークマルウエアペイロード

IoT脅威のトップ

マルウェアのファミリーであるGafgytとMiraiは、当社の調査で圧倒的に多く増殖したIoTマルウェアファミリーのトップ 2でした。実際、当社が観測した900件のユニークペイロードの配布のうち、97％がこの2つのファミリーに属していました。その他のアクティブなファミリーには、Tsunami、VPNFilter、Hajimeがあります。

Gafgytは最もユニークなペイロードを持っていましたが、調査期間中のIoT攻撃では、Miraiマルウェアのペイロードがより頻繁に利用されていました。トランザクション量を見ると、ブロックされた攻撃の76％がMiraiマルウェアファミリーからのもので、5％がGafgyt、19％がその他のマルウェアからのものでした。

IoTボットネット

IoTデバイスを悪用することで、攻撃者はデバイスとそれが接続されたネットワークの両方にアクセスすることができ、あらゆる種類の悪意のある活動が可能になります。特にMiraiとGafgytは、デバイスを利用してボットネットを構築することで知られています。ボットネットは攻撃者のコントロール下にあるデバイスのネットワークで、これにより大規模な協調攻撃が可能になります。ボットネットは、分散型サービス拒否 (DDoS)攻撃、金融データの侵害、暗号通貨の採掘、標的型侵入などに利用されてきました。Miraiボットネットは、2016年に史上最大規模のDDoS攻撃を行い、広範囲に渡ってインターネットの停止を引き起こしたことで知られています。ThreatLabzが、今回のマルウェア調査の一環として、ボットネットコールバックの試みを評価したところ、攻撃者はIoTデバイスだけでなく、人気の高いルーターなどのネットワークデバイスも多数標的にして、これらへの攻撃を実行していることがわかりました。

上位のボットネットコールバックデバイス	
70社以上のベンダーのCCTVとDVR	MVPower DVR
miniigdデーモンでRealtek SDKを使用する複数のデバイス	Linksys デバイス
Huawei HG532	Netgear R7000/R6400デバイス
ZyXELルーター	DGN1000 Netgearルーター
Dasan GPONルーター	D-Linkデバイス
Eir D1000ルーター	Vacron NVRデバイス
D-Linkデバイス	

最も多く標的にされた業界

IoTマルウェアによる攻撃を受けた割合が最も高かったのは技術企業で、感染の40%を占めていました。次に多く標的にされた業界は、製造業 (28%)、小売・卸売業 (24%) でした。

最も多くのマルウェア攻撃を行っている国

当社の調査では、危険にさらされたIoTデバイスの88.5%が、中国 (56%)、米国 (19%)、インド (14%) の3か国のいずれかのサーバーにデータをルーティングしていることが判明しました。これらの国は「マルウェアデスティネーション」として知られており、いずれの場合もマルウェアを直接送信するか、感染後にマルウェアに接続しています。攻撃者の中には、標的としている国の中にコマンド &コントロールサーバーを設置する者もいるため、サーバーの所在地が必ずしも攻撃者の実際の所在地を示すとは限りません。

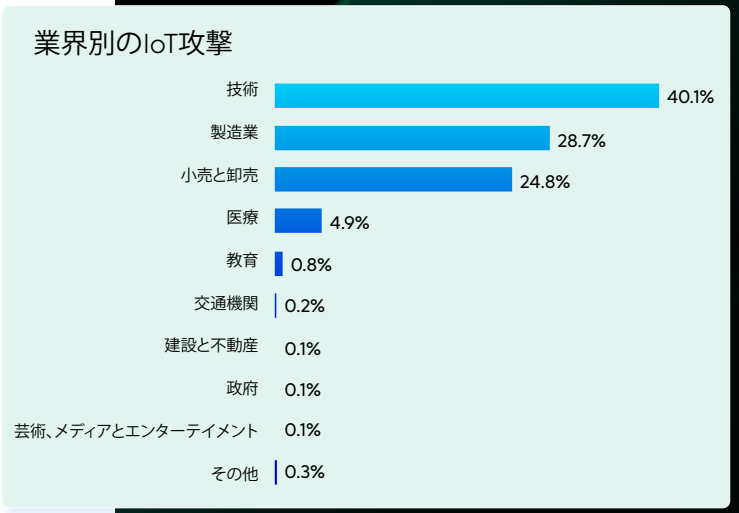


図8：業界別のIoT攻撃

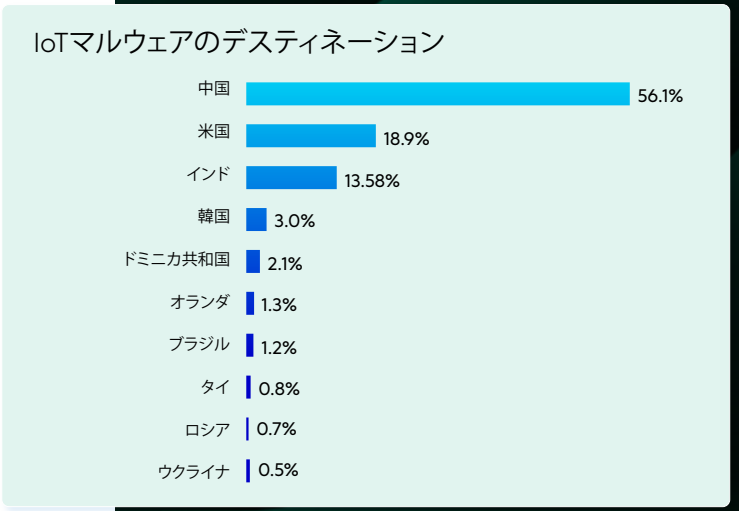


図9：上位のIoTマルウェアデスティネーション

脅威アクターの上位のASN

マルウェアデスティネーションをより詳細に見るために、ThreatLabzがIoTマルウェアに接続していることを確認した上位の自律システム番号（ASN）とIPアドレスをまとめました。

ASN	IP	AS名
16276	158.69.0.77	OVH, FR
398468	193.42.137.107	VMSNETWORKS, US
213035	193.239.147.144	SERVERION-AS Serverion B.V., NL
36352	107.173.125.167	AS-COLOCROSSING, US
202448	86.105.252.203	MVPS https://www.mvps.net,CY
46606	162.241.126.53	UNIFIEDLAYER-AS-1, US
53667	198.251.81.249	PONYNET, US
212953	46.102.106.25	MRS-BILISIM, TR
35913	45.15.143.175	DEDIPATH-LLC, US
213371	37.49.230.52	SQUITTER-NETWORKS, NL
35913	45.15.143.140	DEDIPATH-LLC, US
42864	45.95.169.218	GIGANET-HU GigaNet Internet Service Provider Co, HU
63916	103.42.214.181	IPTELECOM-AS-AP IPTELECOM Global, HK
134520	103.42.214.181	GIGSGIGSCLOUD-AS-AP GigsGigs Network Services, HK
3462	111.248.163.38	HINET Data Communication Business Group, TW
36352	107.173.181.189	AS-COLOCROSSING, US
36352	192.227.147.157	AS-COLOCROSSING, US
212369	45.155.125.116	TRDESERVER, TR
206898	185.172.110.205	BLADESERVERS, AU
213035	193.239.147.245	SERVERION-AS Serverion B.V., NL

図10：脅威アクターの上位のASN

IoTマルウェアの上位の標的

こちらは、クライアントのIPアドレスに基づいて、マルウェアの標的となる「ソース国」です。IoT攻撃の被害を受けた国のトップ3は、アイルランド（48%）、米国（32%）、中国（14%）でした。

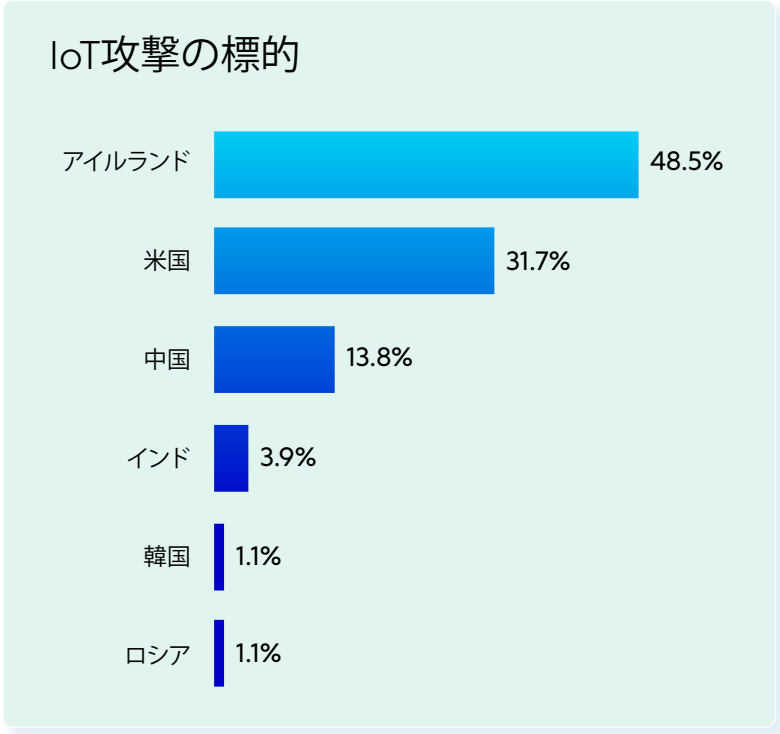


図12：上位のIoTマルウエアソース国

IoTマルウェア感染を防御するための基本事項

世界の「スマート」デバイスには日々新たなものが加わっており、組織内にこれらのデバイスが入るのを阻止することはほぼ不可能です。 そのため、これらのデバイスが機密データやアプリケーションへのオープンドアとならないよう、アクセスポリシーを制定することが重要です。

以下のベストプラクティスは、認可デバイスと非認可デバイスの両方でIoTマルウェアの脅威の低減に寄与します。

→ **ネットワークデバイスを追跡し管理する**
多くのIoTデバイスは管理されていないため、施設内でどのデバイスが使用されているかを可視化するには、エンドポイントエージェントのデータだけに頼ることはできません。 ネットワークログを見て、現在どのデバイスがネットワーク上で通信しているのか、何をしているのかを把握するソリューションを導入した方が良いでしょう。 また、暗号化されたネットワークトラフィックと暗号化されていないワークトラフィックの両方を検査できるアーキテクチャを導入することで、他の方法では気付かないようなデバイスの通信を確認することができます。

→ **デフォルトのパスワードを変更する**
IT業界では古くから言われていることですが、攻撃者がデバイスを悪用する最も簡単で一般的な方法の一つは、デフォルトのパスワードを使用することです。 パスワード管理は、非認可のIoTデバイスでは不可能かもしれませんが、企業が所有するIoTデバイスを導入する際の基本的な第一歩であり、従業員が職場に持ち込むデバイスのセキュリティトレーニングの一環として行うべきものです。

→ **最新のパッチとアップデートを適用する**
多くの業界—特に製造業や医療では—、日々のワークフローの中でIoTデバイスを活用しています。これらの認可デバイスについては、新たに発見された脆弱性を把握し、デバイスのセキュリティに最新のパッチを適用して維持するようにした方が良いでしょう。

→ **ゼロトラストセキュリティアーキテクチャを導入する**
企業資産に厳格なポリシーを適用し、ユーザーやデバイスが必要なものだけ、認証後にアクセスできるようにします。 外部からのアクセスに必要な関連 IP、 ASN、ポートへの通信を制限します。 インターネットへのアクセスを必要とする未認可のIoTデバイスは、トラフィック検査を経て、理想的にはプロキシを介して、すべての企業データからブロックされるべきです。 企業ネットワークに脅威をもたらすシャドー IoTデバイスを阻止する唯一の方法は、暗黙の信頼ポリシーを排除し、 —ゼロトラストとも呼ばれる動的なIDベース認証を使用して機密データへのアクセスを厳密に制御することです。

ThreatLabZについて

ThreatLabZは、ゼットスケーラーのセキュリティ研究部門です。ワールドクラスのこの研究部門は、新たな脅威を発見し、ゼットスケーラーゼロトラストエクスチェンジのグローバルプラットフォームを使用する何千もの組織を常に保護する、重要な役割を担っています。マルウェアの調査と行動分析に加え、ゼットスケーラーのプラットフォームの高度な脅威保護の新しいプロトタイプモジュールの研究開発も進めており、社内のセキュリティ監査を定期的に実施することで、ゼットスケーラーの製品やインフラストラクチャがセキュリティコンプライアンス基準を満たしていることを確認しています。ThreatLabZは、新たな脅威の詳細分析を定期的にポータルで（research.zscaler.com）で公開しています。

ゼットスケーラーについて

ゼットスケーラーは、デジタルトランスフォーメーションを加速させ、俊敏性、効率性、耐障害性、安全性の向上を可能にします。ゼットスケーラーのゼロトラストエクスチェンジは、あらゆる場所のユーザ、デバイス、アプリケーションを安全に接続することで、サイバー攻撃やデータ損失から何千ものお客様を保護しています。SASEベースのゼロトラストエクスチェンジは、世界中の150以上のデータセンタに分散する、世界最大のインラインクラウドセキュリティプラットフォームです。詳細は、**zscaler.jp**をご覧ください。