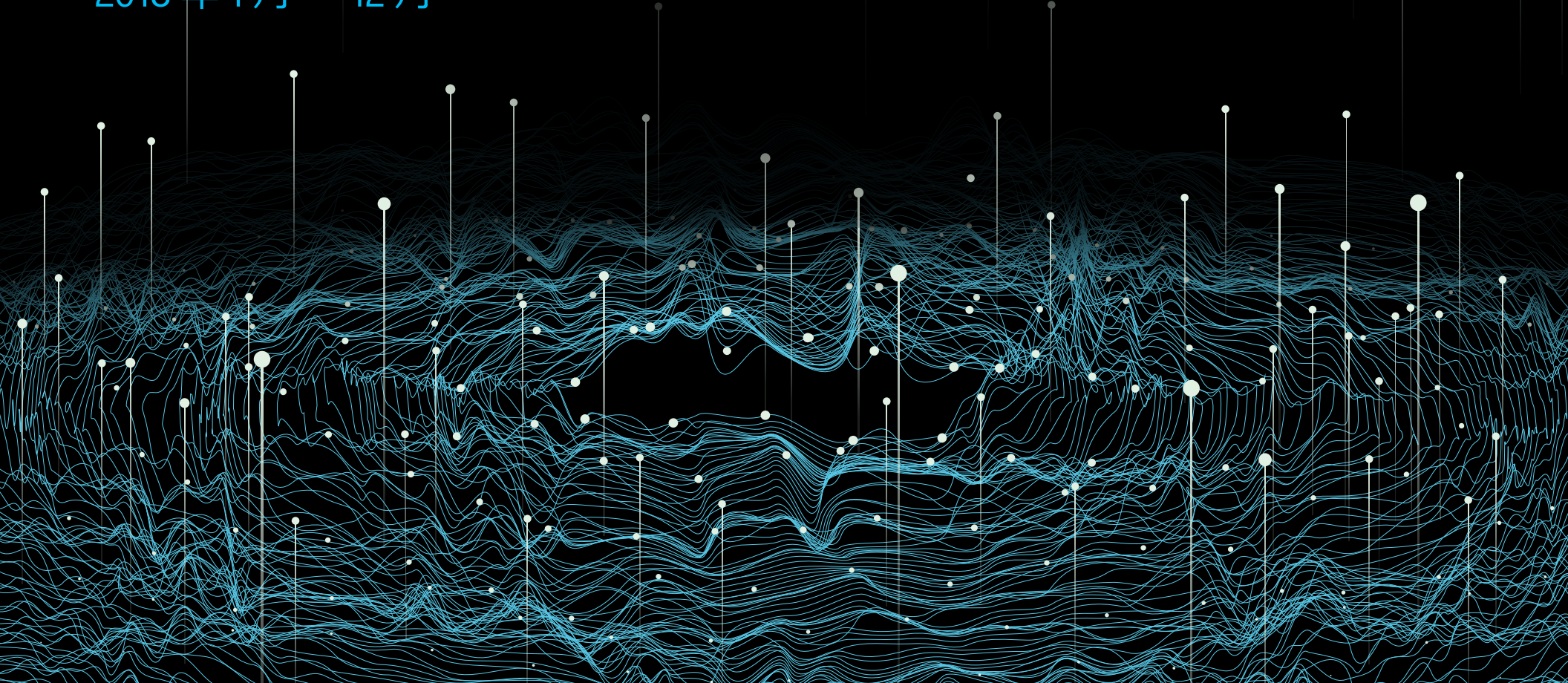




マイクロソフト セキュリティ インテリジェンス レポート

第 24 版

2018 年 1 月 ~ 12 月



目次

この文書は情報提供のみを目的としています。Microsoft は、本書に記載された情報について、明示的、黙示的、または法的保証を一切いたしません。

このドキュメントは現状有姿で提供されます。このドキュメントに記載されている情報 (URL などのインターネット Web サイトに関する情報を含む) は、将来予告なしに変更されることがあります。このドキュメントの使用に起因するリスクは、利用者が負うものとします。

Copyright © 2019 Microsoft Corporation. All rights reserved.

このドキュメントに記載されている実在する企業名および製品名は各社の商標です。

著者および寄稿者

Abhishek Agrawal

情報の保護

David Fantham

情報の保護

Debraj Ghosh

Microsoft Security Marketing

Diana Kelley

Cybersecurity Solutions Group

Elia Florio

Windows Active Defense

Eric Avena

Windows Defender Research Team

Eric Douglas

Windows Defender Research Team

Francis Tan Seng

Windows Defender Research Team

Jonathan Trull

Cybersecurity Solutions Group

Joram Borenstein

Cybersecurity Solutions Group

Karthik Selvaraj

Windows Defender Research Team

Kasia Kaplinska

Microsoft Security Marketing

Kristina Laidler

Security Incident Response

Matt Duncan

Windows Active Defense Data Engineering および Analytic

Mark Simos

Cybersecurity Solutions Group

Paul Henry

Wadeware LLC

Pragya Pandey

Microsoft Security Marketing

Ram Pliskin

Azure Security

Ryan McGee

Microsoft Security Marketing

Seema Kathuria

Cybersecurity Solutions Group

Steve Wacker

Wadeware LLC

Tanmay Ganacharya

Windows Defender Research Team

Volv Grebennikov

Bing

Yaniv Zohar

Azure Security

はじめに

マイクロソフト セキュリティ インテリジェンス レポート (SIR) 第 24 版によろこそ実務者およびセキュリティ アーキテクトとして、私はこのようなレポートを読み、その知識を活用して、組織をより効果的に防御および保護する方法に関する実用的なアドバイスを持ち帰って、その概況を少しでもよく理解したいと望んでいます。

このレポートには、サイバー レジリエンスの改善状況を伝えようとする SIR チームの理念と、1 年間蓄積・精査されたデータから得られた最も重要な教訓が詰まっています。

今お読みになっているものは、1 年間のセキュリティ データ分析および実地訓練で学習され、選り抜かれたインサイトです。分析データは、日々マイクロソフトのクラウドを通過する 6.5 兆におよぶ脅威の兆候と、世界中の数千のセキュリティ研究者と応答者から寄せられる研究結果および現場での知見で構成されています。攻撃者は 2018 年も、最新型的手段と従来の手段を組み合わせ、お客様や組織のデータとリソースを盗もうと模索し続けていました。最新型的手段とは通貨マイニング、従来の手段とはフィッシングを指します。また、Ursnif キャンペーンに代表されるソーシャル手法と技術的手法を組み合わせたハイブリッド型の攻撃も目立ちました。攻撃の形態が騒がしくて破壊的なランサムウェアに対して、防御者が賢明な対応するようになるにつれ、犯罪者はより「人目につきにくい」が、儲けが大きいコインマイナーに軸足を移しています。

このような旋回は、攻撃者が常に一歩先んじているようで、いらいらさせられるかもしれません。ただし、別の視点から見れば、今回の変化は望ましい動きだと言うこともできます。あなたのような防御者やサイバーセキュリティの専門家は、攻撃者に好みのペイロードを変更させ、ランサムウェアから撤退させる防御的なテクニックを実装しました。

サイバー犯罪者が活動を増やしているもう 1 つの領域は、サプライ チェーンです。最も顕著なのが、1 件のピアツーピア アプリの感染によって 2018 年 3 月 6 日に発生した、Dofail コインマイナーの蔓延です。サプライ チェーンの場合、悪意のあるブラウザ拡張機能、Linux リポジトリの侵害、複数のモジュールのバックドア感染など、懸念の範囲はアプリにとどまらずクラウドにまで及びます。この脅威に対処するために、サプライ チェーン モデルの透明性と信頼性の向上が進められつつあります。

データは重大なものですが、組織で実際に何が起きたかを発見する際に、役立つこともあります。こうしたことから、今回のレポートでは、マイクロソフトの Detection and Response Team (DART) が実際の現場で得た教訓を記載しています。この中には、大製造企業が、数か月にわたって蔓延した多層のフィッシング キャンペーンをブロックするために、いかにコントロールを実装したか、また高度な調査ツールとエンドポイント モニタリングを使用して、システムから脅威アクターを最終的に絶滅できた、金融サービス組織の例が含まれています。

最後にまとめてみます。フィッシング クリックは増加し続けましたが、マシン ラーニング モデルは、そのクリックがユーザー ボックスをヒットする前に、フィッシュをうまくキャッチできるようになり、クリックされても危害を防止できるようになりました。さらに心強いのは、さらに多くの会社が、信用情報窃盗フィッシング電子メールの成功を制限する、マルチファクター ソリューションを実装していることです。

攻撃者は機会をうかがっているため、彼らのテクニックやスパイ技術を知れば知るほど、より良い準備をして防御を構築し、素早く対応できるようになります。小さな取り組みを積み重ねることで、サイバーセキュリティの健全性を組織全体で高めることが可能になります。このレポートでは、マルウェアや攻撃における変化に関する最新の知見に加え、推奨される手順、マイクロソフトが提案するベスト プラクティスをご確認いただけます。これらの情報は、私が現場担当者として攻撃者に対峙するときに、まさに必要としているものばかりです。皆さんにもきっとお役立ていただけると信じています。

Diana Kelley

マイクロソフト サイバーセキュリティ フィールド CTO

追伸私たちは SIR をいかに改善するか常に模索しています。フィードバックを受信したら、手を差し伸ばしてその方法を教えてください。



セクションI

ランサムウェア、 仮想通貨マイニング、 およびマネー

2017 年の重大なセキュリティ ストーリーには、その多くにランサムウェアが含まれていました。WannaCrypt および Petya thrust ランサムウェア (コンピューターをロックまたは暗号化し、アクセスを回復するにあたり金を要求する、マルウェアの一種) は世界中で猛威をふるいました。また多くの人が、同様の脅威は今後拡大しても減少することはないと予想していました。ただし、ランサムウェアとの遭遇は 2018 年には大幅に減少しました。

ランサムウェアとの遭遇が減少した要因は、部分的には、検知能力と教育の向上により、攻撃者が恩恵を得にくくなったことがありました。この結果、攻撃者の注目はランサムウェアから仮想通貨マイニングなどのアプローチにシフトし始めました。これは、ユーザーのコンピューティング リソースを盗用して、攻撃者のためのデジタル マネーを生み出す手法です。このシフトは、サイバー犯罪者の基本的に日和見主義的な性格を表すものです。つまり、最も簡単に手に入るお金を追求める傾向があり、サイバー犯罪の経済性が変われば、すぐそれに追随することになります。

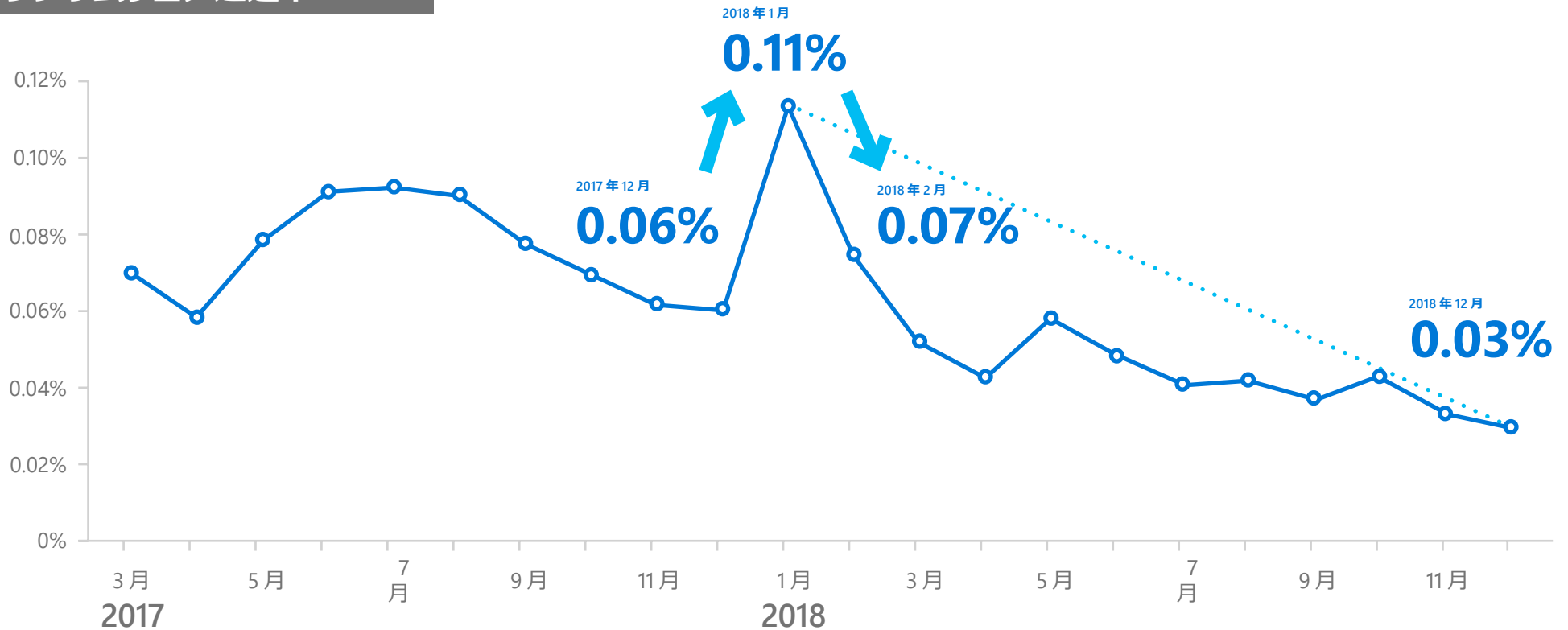
ランサムウェア攻撃は減少傾向

10 年以上前にマルウェア アンダーグラウンドを占領していたハッカーやいたずら者は、組織犯罪やその他の営利目的に取って代わられました。初期のマルウェアの蔓延は、しばしば一時的で明瞭なものでしたが、利益志向のマルウェアは、その機能 (スパムの送信、機密情報の窃盗、サービス拒絶攻撃の実行、およびその他の悪意のある活動) の続行のために、できる限り穏やかに動作し、注意の喚起を避けました。

ランサムウェアはこの傾向に抵抗しました。ランサムウェアは、検知されないことを目指すのとは逆で、被害者が身代金を払うまで、彼らのコンピューターにアクセスすることを目に見える形で拒絶します (身代金を支払った後も攻撃者がコンピューターの制御権を引き渡さないケースも多くあります)。ランサムウェアのピークは

2017 年でしたが、このようなオープン型攻撃が登場したことは、攻撃者の技術が新たな段階に達したことを示しているように思われました。一方、直近のデータは、ランサムウェアが減少傾向にあることを示しています。攻撃者が仮想通貨マイニングなどの攻撃をより効果的に実行するため、過去の潜伏型の動作を再び採用し、できる限り捕捉されないことを目指しているということです。ランサムウェアとの遭遇率は減少傾向にありますが、これで攻撃の重大度が減少しているとは、必ずしも言えません。

ランサムウェア遭遇率



ランサムウェアとの遭遇率は、2017年3月と2018年12月の間で、**およそ60%減少しましたが**、その期間で断続的には増加しました。

▲ 図1

ランサムウェアとの遭遇率 (2017年3月～2018年12月)

この全体的な減少傾向には多くの原因が考えられますが、マイクロソフトのセキュリティ研究者は、主要な要因が、エンドユーザーと組織の両方がランサムウェアの脅威をより認識して、よりインテリジェントに対応しているためと考えています。こうした対応の中には、より大きな注意を払い、重要なファイルをバックアップして、ランサムウェアによって暗号化されても、復元できるようにしたことがあります。また、以前にお話したように、サイバー犯罪者は楽天的でもあります。

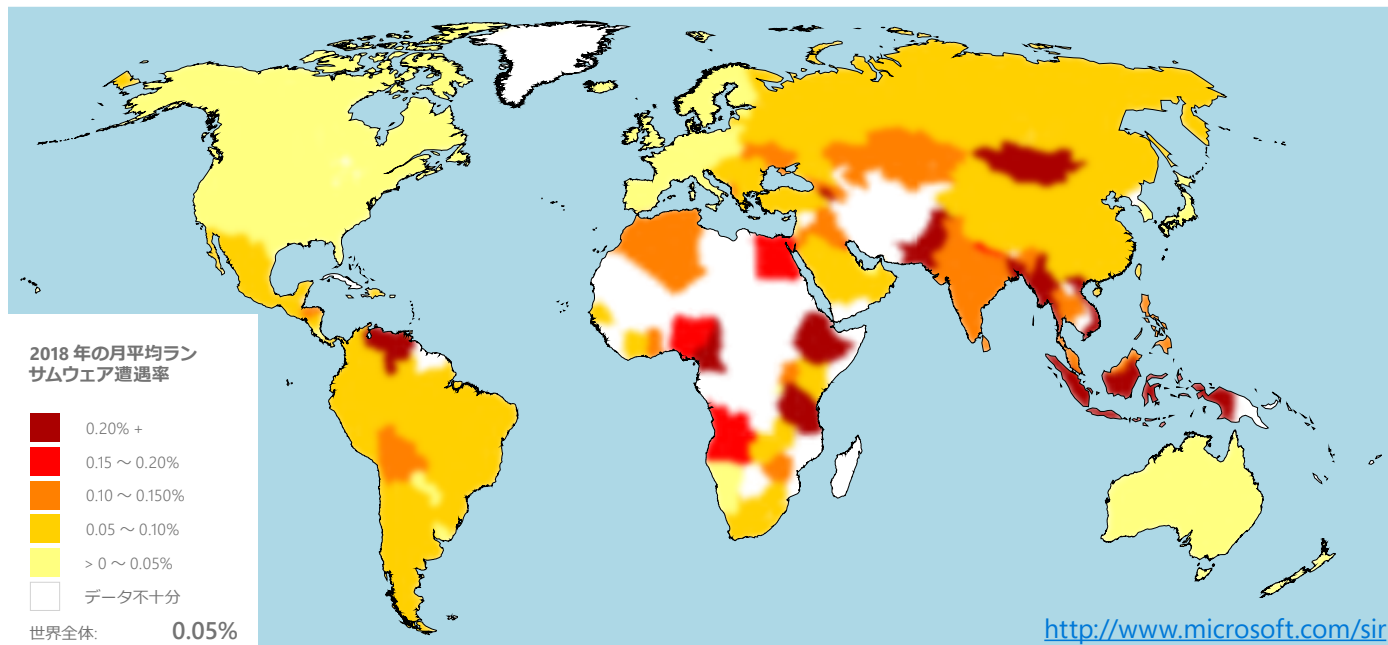


図 2

2018 年の全世界の月平均ランサムウェア遭遇率 (国/地域別)

ランサムウェアの影響を最も受けた国:
エチオピア



月平均の遭遇率:

0.77%

2018 年の月平均ランサムウェア遭遇率が高かった上位 5 つの場所は、エチオピア (0.77 %: 月平均のランサムウェア遭遇率)、モンゴル (0.46)、カメルーン (0.41)、ミャンマー (0.33)、およびベナズエラ (0.31) で、それぞれの月平均ランサムウェア遭遇率は、当該期間中 0.31 % 以上でした。1 数年前までは、ランサムウェアとの遭遇は、ヨーロッパや北米などの裕福な国や地域に集中していましたが、ランサムウェアが攻撃者の寵愛を失い始めると共に、遭遇パターンは全体としてマルウェアのそれと極めて類似してきました。

2018 年にランサムウェア遭遇率が低かった場所は、アイルランド (0.01)、日本 (0.01)、米国 (0.02)、英国 (0.02)、およびスウェーデン (0.02 %) で、それぞれの月平均遭遇率は、当該期間中 0.02 % 以下でした。遭遇率が低い場所には、成熟したサイバーセキュリティ インフラストラクチャー、およびクリティカルなインフラストラクチャーを保護し、基本的なセキュリティに関して市民と対話するための十分に確立されたプログラムがある傾向があります。

脚注

¹ 遭遇率とは、マイクロソフト リアルタイム セキュリティ製品を実行しているコンピューターの中で、マルウェアとの遭遇を報告しているものの割合です。脅威に遭遇しても、コンピューターが感染したわけではありません。マイクロソフトへのデータ提供に同意したユーザーのコンピューターのみが、遭遇率の計算時に考慮されています。

増加する仮想通貨マイニング

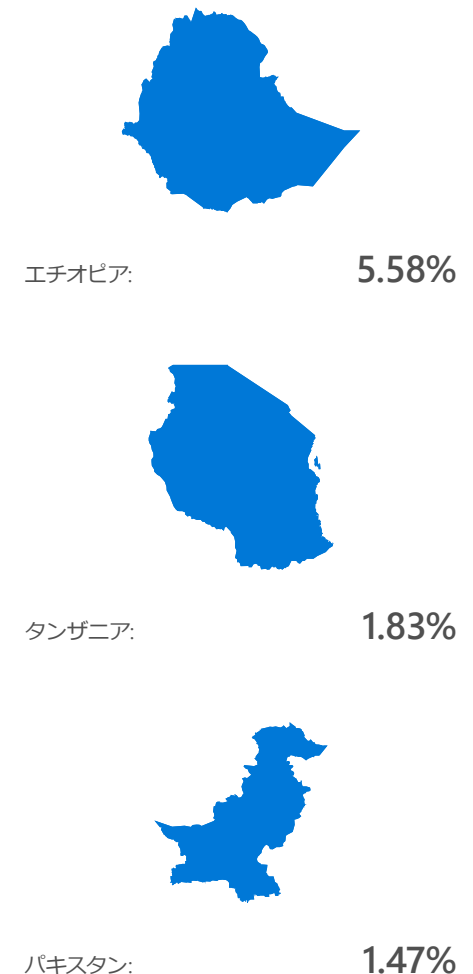
仮想通貨とは、商品やサービスをオンラインや現実世界で、匿名で購入および販売する際に使用できる、仮想通貨のことです。多数の各種仮想通貨が存在しますが、すべてがブロックチェーンテクノロジーに基づいています。このテクノロジーではすべての取引が分散台帳に記録され、この分散台帳が、世界中の数千または数百万のコンピューターによって保守されています。新しいコインは、コンピューターの複雑な計算によって作成（採掘）されます。これらのコンピューターが、ブロックチェーン取引を検証する役割も担っています。

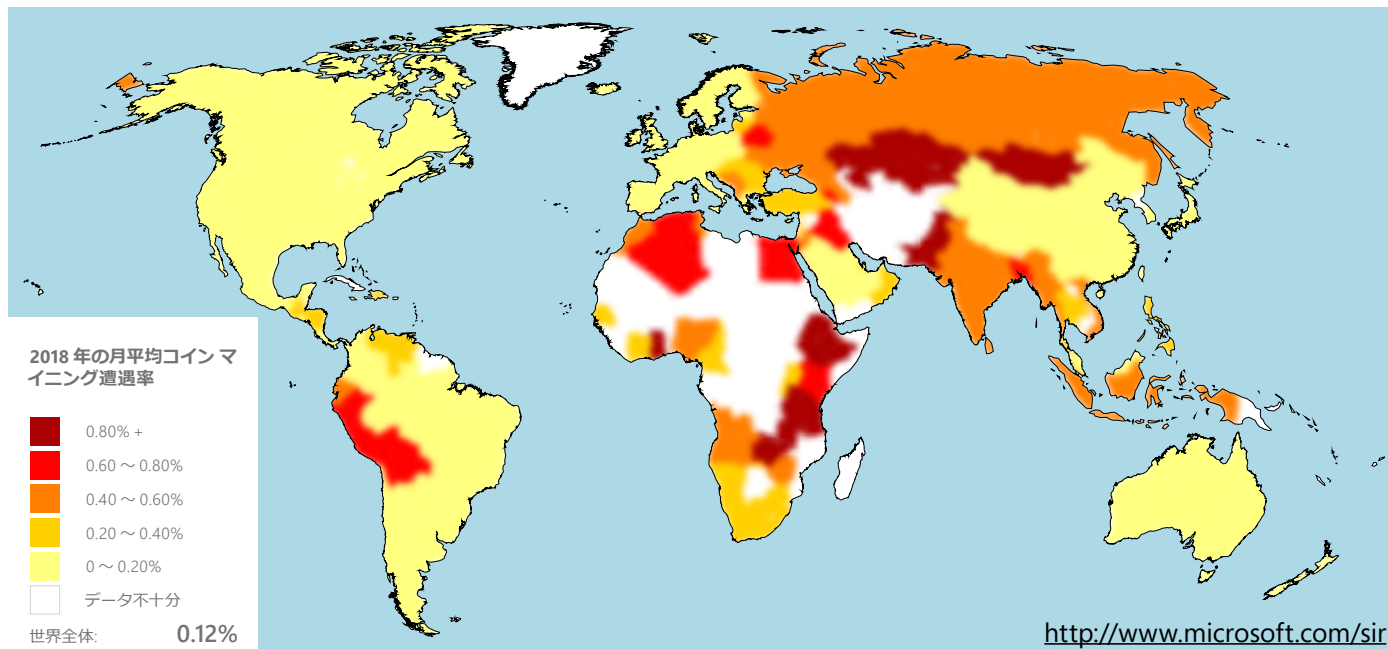
コインのマイニングは非常にもうかる - 2018 年には、たった1つのビットコイン（最も古く最も普及した仮想通貨）の価値が数千 US ドルになりましたが、それに必要な計算の実行は、非常にリソース インテンシブになる可能性があります。新しいコインが採掘されるたびに、さらにその傾向が強まります。Bitcoin などの普及している通貨の場合、巨大なコンピューティング リソースにアクセスせずに利益を上げるとはほとんど不可能であり、そのようなリソースは、個人や小規模なグループでは利用できません。このため、マルウェアを介してコンピューターを操り、自らの仮想通貨の採掘を肩代わりさせ、不正に利益を上げようとする攻撃者がますます増えてきました。この手法を使えば、攻撃者は、1 台や 2 台のコンピューターでなく、数十万台のコンピューターの処理能力を利用できるのです。わずかな感染が見つかって、仮想通貨の匿名性のため、該当者を追跡する労力が複雑化します。

2018 年には、仮想通貨コイン マイニングの遭遇率は、ランサムウェアのたった 0.05 % に比べて 0.12 % でした。マイニングがこれほど普及した要因には、マルウェアが必要とする処理も大きく関係しています。ランサムウェアとは違い、仮想通貨マイニングではユーザーによる入力が必要です。ユーザーが他のタスクを実行していたり、コンピューターから離れていたたりする間もバックグラウンドで動作するため、コンピューターのパフォーマンスがかなり低下するまで、まったく気付かれない可能性があります。結果として、マイニングの脅威を取り除くための対策が一切講じられないまま放置される可能性があります。ユーザーのマイニング時間が長くなればなるほど、攻撃者の利益は増大します。

多数の仮想通貨の人目につかないマイニング用の「既成」製品の可用性は、こうした傾向のもう1つの駆動力となります。サイバー犯罪者は、この手軽さを利用します。どこでも手に入るコイン マイニング ソフトウェアを再パッケージして、疑いを持たないユーザーのコンピューターに送り込んでいます。悪意に基づいて武器化されたマイニング ソフトウェア（マイナー）は、ソーシャル エンジニアリング、脆弱性の悪用、ドライブバイ ダウンロードなど、その他の脅威とも共通・類似する手法によって被害者のコンピューターに潜入します。インストールされたマイニング ソフトウェアは被害者のコンピューターのバックグラウンドで実行され、ブロックチェーン計算を実行して、発生した報酬は攻撃者が奪い去るというわけです。

仮想通貨マイニングの影響を最も受けた国の月平均遭遇率





◀ 図 3

2018 年の全世界の月平均コインマイナー遭遇率 (国/地域別)

仮想通貨マイニングの影響が最も少なかった国の月平均遭遇率



アイルランド:

0.02%



日本:

0.02%



米国:

0.02%

2018 年に仮想通貨コイン マイニングの遭遇率が高かった 5 つの国は、エチオピア (5.58)、タンザニア (1.83)、パキスタン (1.47)、カザフスタン (1.24)、およびザンビア (1.13 %) で、それぞれの月平均遭遇率は、当該期間中ほぼ 1.13 % 以上でした。2018 年にコイン マイニング遭遇率が低かった場所は、アイルランド、日本、米国、中国で、それぞれの月平均のコイン マイニング遭遇率は、当該期間中ほぼ 0.02 % でした。

新たな脅威: ブラウザーベースの仮想通貨マイニング

このセクションで示す統計には、犠牲者のコンピューターにマルウェアとしてインストールされる悪意のある仮想通貨マイナーが含まれています。ただし、最も影響力のある仮想通貨マイニングによる脅威の中には、インストールの必要がまったくなく、完全に Web ブラウザー内で完結するものもあります。実際、Web サイトの所有者が広告に頼らずサイトトラフィックを収益化する方法として、ブラウザーベースの仮想通貨マイニングを宣伝するサービスは数多く存在します。この場合サイト所有者は、サイト訪問中のユーザーのバックグラウンドで仮想通貨をマイニングする JavaScript コードを、所有ページに追加します。収益はサイト所有者とサービスの間で分け合います。残念なことに、こうしたサービスはすぐに攻撃者に悪用されることになりました。具体的には、合法的な Web サイトに侵入してマイニングコードをソースコードに挿入し、

Brocoiner 遭遇率



エンドユーザーの同意を得ずに仮想通貨を採掘します。ブラウザベースのマイナーは、コンピュータの性能を著しく低下させ、感染した Web ページにアクセスするユーザーの電力を浪費します。仮想通貨マイニングのトロイの木馬のように、ブラウザベースのマイナーは、コンピュータの性能を著しく劣化させ、ユーザーが対象 Web ページにアクセス中に、電力を浪費します。

図 4

Brocoiner (最も蔓延しているブラウザベースの仮想通貨マイナー) の遭遇率

未承諾で実行される仮想通貨マイニングの影響

仮想通貨マイニングの犠牲者が直面する最も明白な脅威は、コンピュータ リソースの浪費であり、電力を浪費し、コンピュータの性能を著しく劣化させます。また、ユーザーと組織は、コイン マイニングから以下を含むその他のリスクにも直面します。

- 1 今後の被害拡大の「足掛かり」を築かれる。**

他のマルウェアの形態と同様に、仮想通貨マイニングは攻撃者のエントリポイントになる可能性があります。コンピュータがバックグラウンドで仮想通貨をマイニングしている間に、サイバー犯罪者が環境の情報を収集してセキュリティギャップを特定し、別の目的のために悪用する可能性があります。
- 1 侵入されたインターネット接続デバイスが、仮想通貨マイニングのボットとして悪用される。**

マルウェア脅威検知などのビルトインセキュリティを持たない数多くのインターネット接続デバイスは、攻撃者の格好のターゲットになる可能性があります。
- 1 マシンの物理的被害。**

何か月も継続的に動作する仮想通貨マイニングソフトウェアは、パフォーマンスを低下させるのはもちろん、過剰な電力消費と CPU 利用が生成する熱によりコンピュータに物理的な被害を与える可能性があります。



セクションⅡ

危険にさらされる ソフトウェア サプライチェーン

数年にわたって、マイクロソフトでは、攻撃のエントリーポイントとして[サプライチェーン危険化](#)を使用する、脅威実行者を追跡しています。サプライチェーン攻撃では、攻撃者は、正規のソフトウェア発行者の開発または更新プロセスへの侵入に注力します。

これに成功すると、攻撃者は感染したコンポーネントを正規のアプリケーションや更新パッケージに組み込むことができ、その後、ソフトウェアのユーザーに分配されます。侵害されたソフトウェアが持つ信頼性と権限で、悪意のあるコードが実行されます。[ここ数年間のソフトウェアサプライチェーン攻撃](#)は、サイバーセキュリティに関する多くの会話で重要なトピックとなり、多くのIT部門の主要な関心事になっています。



2017 年の主なソフトウェア サプライチェーン攻撃

2017 年には、サプライチェーン攻撃が注目を浴びたインシデントとなり、最も注目されたものとして、6月の[Petya ランサムウェアの蔓延](#)がありました。これをトレースしたところ、初期感染は、ウクライナの一般的な税務会計アプリケーション用の更新プロセスが侵害されたことがわかりました。5月には、[Operation WilySupply](#) が、テキストエディターのソフトウェア更新プログラムを侵害して、金融およびITセクターのターゲット組織にバックドアをインストールしました。7月には、[ShadowPad](#) と呼ばれるバックドアが、サーバー管理ソフトウェアパッケージに隠され、攻撃者が、データ窃盗およびその他の悪意のある活動用に、追加のマルウェアペイロードをインストールできるようになりました。9月には、一般的なフリーウェアツール CCleaner のインフラストラクチャーが侵害され、[バックドアバージョン](#)がそのユーザーベースに配信されました。

▲ 図 5

2017 年および 2018 年のソフトウェア サプライチェーン攻撃

2018 年のソフトウェア サプライ チェーン攻撃 – 根本原因とその影響

2018 年の最初の主要なサプライ チェーン攻撃インシデントは、3 月 6 日に発生しました。このとき、Windows Defender ATP は、Dofail trojan (Smoke Loader と呼ばれる) を配信する大規模なキャンペーンをブロックしました。この大量のマルウェア キャンペーンは、感染したピアツーピア アプリケーションまでトレースされました。このアプリケーションの更新パッケージが悪意あるパッケージに置き換えられていたことで、悪意あるパッケージが侵害用コードをダウンロードし、その後 Dofail マルウェアをインストールしていたのです。この最新型のトロイの木馬には、コイン マイニング ペイロードが仕込まれていました。この手法には、高度なクロスプロセス インジェクション、永続化メカニズム、検出回避など、さまざまな技術が駆使されていました。

▼ 図 6

2018 年 3 月の Dofail (Smoke Loader) 遭遇率の増加は、インスタンスのブロック数が急増したことを示す

Dofail 遭遇率



キャンペーンの最初の 12 時間で、Windows Defender Antivirus は、**世界中で 400,000 を超える感染をブロックしました。**ロシアは全世界の遭遇率の 73 % を占め、その後、トルコとウクライナがそれぞれ 18 %、4 % で続きます。

2018 年には、次の表に示すような、侵害したソフトウェア サプライ チェーンを配信手段として利用する攻撃が新たに検出されました。

期間	攻撃	説明	感染ソフトウェア
2018 年 3 月	Dofoil コイン マイニング キャンペーン (報告者: マイクロソフト)。	攻撃者はピアツーピア アプリの更新プロセスに侵入、Dofoil をインストールして、さらに Dofoil がコイン マイニング マルウェアをインストールしました。	ピアツーピアのアプリ
2018 年 7 月	サプライ チェーン内で侵害されたサプライ チェーン (報告者: マイクロソフト)	攻撃者は、PDF エディター アプリ ベンダーと同社のソフトウェア ベンダー パートナーが共有するインフラストラクチャーを侵害しました。	PDF エディター アプリとサードパーティ パートナー ベンダー。
2018 年 8 月	侵害されたリモート サポート プログラム (Red Signature 作戦、報告者 Trend Micro および IssueMakersLab)。	リモート サポート ソリューション プロバイダーの更新サーバーが侵害され、9002 RAT と呼ばれるリモート アクセス ツールが配信されました。	リモート サポート プログラム。
2018 年 10 月	侵害されたホスティング コントロール パネル ソリューション (報告者: ESET)	ホスティング コントロール パネル ソリューションのインストール スクリプトが、資格情報を盗むよう書き換えられました。	ホスティング コントロール パネル ソリューション

◀ 図 7

2018 年のその他のソフトウェア サプライ チェーン攻撃

危機にさらされる信頼性

サプライ チェーン攻撃は、使用しているソフトウェアに対して置いているユーザーと IT 部門の信頼を悪用しているため、陰湿です。侵害されたソフトウェアの多くはベンダーにより署名・認証されているため、不自然な兆候が顕在化しにくく、感染の検知はきわめて困難です。サプライ チェーン攻撃は、サプライ チェーンとその顧客 (法人、個人を問わず) 間の信頼関係を毀損します。また、ソフトウェアを汚染し、配信・更新のインフラストラクチャーを弱体化することで、組織が提供する商品とサービスの完全性と安全性を損ないます。

サプライ チェーン攻撃は、広範なソフトウェアと様々なセクターと地理的場所にある対象組織に影響を与えます。サプライ チェーン攻撃の脅威は、業界全体の問題で、コードを作成するソフトウェア開発者とベンダー、ソフトウェアのインストールを管理するシステム管理者、これらの攻撃を見つけ、それらから人々とソフトウェアを保護するソリューションを作成する情報セキュリティコミュニティを含めた、複数の株主の注意が必要となります。

ソフトウェア以外の経路: クラウド オブジェクトを悪用するサプライ チェーン侵害

信頼の土台を壊すサプライ チェーン攻撃の能力は、クラウドで増幅され、より複雑になります。2018 年の侵害されたクラウド オブジェクト、サービス、およびインフラストラクチャーのいくつかのインシデントでは、この複雑さがハイライトされています:

- クリック詐欺マルウェアをインストールした毒入りの Chrome 拡張 (報告者: [ICEBRG](#))
- Linux リポジトリの各種の侵害 (報告者: 複数のオンライン フォーラム)
- 攻撃者が WordPress サイトでコンテンツを公開可能にするものを含め、様々な悪意のあるアクティビティで使用される、悪意のある WordPress プラグイン (報告者: [Wordfence](#))
- 仮想通貨コイン マイニング マルチをダウンロードし、Docker Hub アカウントにアップロードしたスクリプトを含む、悪意のある Docker イメージ ([Fortinet](#) および [Kromtech](#) による報告)
- 公式な Python リポジトリ内のタイポスクワッティングな悪意のあるパッケージ; クリップボード内のコイン マイニング アドレスをハイジャックするために使用されるマルウェアをダウンロードする悪意のあるスクリプトを含むパッケージ ([中間](#)で報告された)
- 攻撃者が StatCounter を使用している Web サイト内に悪意のあるスクリプトの注入を許した、StatCounter 内の侵害されたスクリプト ([ESET](#) によって報告された)

- 裏切られた npm モジュールの複数のインシデント ([npm ブログ](#), [中間](#)) これは、エクスプロイトされた場合、例えば、攻撃者が任意のコードを実行中のサーバーに入力して、実行できるなどの状況を引き起こす可能性がある

これらのインシデントは、サプライ チェーン危険化がいかに途方もなく攻撃面を広げられるかを示します。保護されていないクラウド オブジェクトは、攻撃の経路として予期せず利用される可能性があります。たとえば Docker Hub のインシデントの場合、悪意のあるアカウントによって、コイン マイニング バックドアが仕込まれた Docker イメージがアップロードされました。Docker イメージは、ほぼ 1 年間 Docker Hub 上でホストされ、数百万回もダウンロードされ、何も疑っていない管理者やユーザーによって使用されました。

サプライ チェーンのリスクは、クラウド、オープン ソース、Web サイト ライブラリ、コンテナ内のコードやクラウド内の他のオブジェクトにまで拡張されます。その一方で、ソフトウェアとハードウェアのサプライ チェーンを対象とした侵害のインシデントはますます多様化しています。このようなリスクと侵害の多様化により、サプライ チェーン攻撃の脅威カテゴリとしての重大性が高まっています。こうした種類の攻撃の全領域に対する単一のソリューションはありませんが、組織では、侵害されたハードウェアおよびソフトウェアのサプライヤー、ベンダーと買収、オープン ソースのソフトウェア サプライヤー、およびクラウド サービスとインフラストラクチャーのサプライヤーからのサプライ チェーン攻撃の[予防的保護と侵害後の検知](#)を構築する必要があります。

DART によるサイバー インシデント調査

Microsoft Detection and Response Team (DART) は、サイバーセキュリティ インシデントに対する検知、調査、および対応で組織を支援する、サイバーセキュリティ エキスパートとインシデント応答者のグローバル チームです。このセクションでは、DART が昨年対応したお客様のいくつかのケースをハイライトします。一般的な攻撃者の傾向、およびマイクロソフトとお客様がこれらをいかに削減できたかを図示します。

プロフェッショナル サービス組織が遭遇した、国家支援によるデータ不正取得攻撃

専門的サービス組織では、データを密かに抽出した民族国家攻撃を経験しました。組織の資格情報に特権アクセスする、洗練された州が提案する先進の持続的脅威 (APT) に感染しました。攻撃者はパスワード スプレー攻撃を使用してネットワーク アクセスを取得。多数のユーザー アカウントをターゲットに、安全性の低いパスワードや広く使用されているパスワード (“p@ssword” や “123456” など) をいくつか試行して、Office 365 の管理者資格情報を取得しました (パスワード スプレー攻撃は、各アカウントに対するログイン試行数を抑えることで検知を回避します)。ネットワークに潜入した APT は、従業員のメールボックスから、データの不正取得を自動実行しました。組織内でも APT を強制排除する措置が何度も試みられましたが、攻撃者は 200 日以上もネットワークにとどまり、攻撃の一環として、相手は組織のサプライチェーン ソフトウェアを利用して、データの抽出を自動化しました。

彼らは顧客データの漏洩を疑っていたため、組織は DART チームと連携して、さらなる損害を調査し、防止に役立てました。DART は、対象となった Office 365 メールボックス検索、侵害されたアカウント、攻撃者のコマンド アンド コントロール チャネルを特定しました。このインシデントを通してお客様が得たのは、クラウド サービスを ID ベースの脅威や攻撃者から保護するためのコントロールをデプロイしなければならないという重要な教訓です。このため同組織では、多要素認証 (MFA)、特定のクラウド アプリに対する条件付きアクセス ポリシー、Office 365 のログ記録を導入しました。さらに Endpoint Detection and Response (EDR) ソリューションを導入すれば、攻撃者によるネットワーク不正利用の試みを検知し、今後同様の脅威に対するセキュリティを強化することもできます。さらに、我々は、この組織が、適切なユーザー認証ポリシーを管理および強制する、クラ

ウド ガバナンス主体またグローバル アイデンティティ チームを指名して、組織がセキュリティ姿勢を監視し、リスクを効果的に緩和できるようにしました。



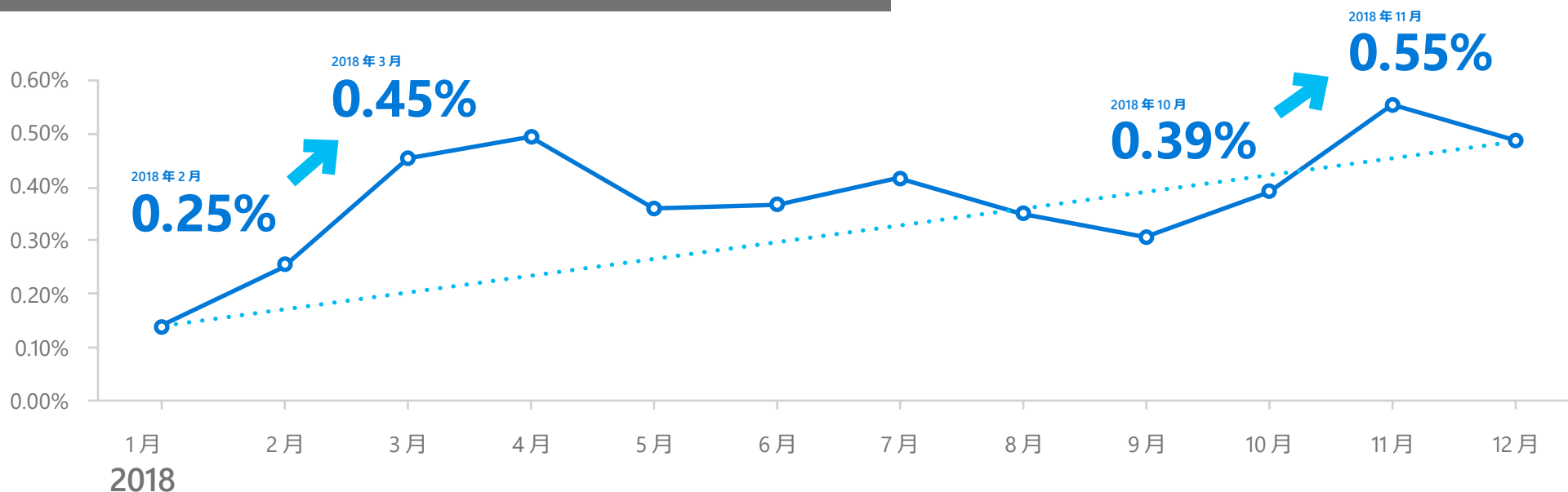


セクション III

フィッシングは
まだ流行している

2018 年に、マイクロソフトの脅威アナリストは、**攻撃者が依然フィッシングを好み**
の攻撃方法として使用し続けているという証拠を確認しています。フィッシング
は、犠牲者を自分の餌にしようとするサイバー犯罪者の永続的な努力の前で、人間の
決定と判断に関わるため、予見可能な将来にわたって問題として残ります。

依然上昇するフィッシングレート フィッシングメールの総着信メールに占める割合



2018 年も、フィッシングは有力な攻撃手法

マイクロソフトでは、Office 365 の毎月 4700 億以上の E メール メッセージで、フィッシングやマルウェアを解析およびスキ
ャンしており、これがアナリストに攻撃者の傾向とテクニックに対する相当なインサイトを提供しています。フィッシング
メッセージであった着信 E メール の割合は、2018 年 1 月 ~ 12 月の間で **250 % 増加** しました。フィッシングは、悪意のあるゼ
ロ日ペイロードをユーザーに配信するために使用された上位攻撃ベクトルの 1 つとして残り、マイクロソフトでは、これらの
攻撃に対して、ユーザーの安全を確保するため、追加のフィッシング対策保護、検出、調査、および応答機能で、対抗し続け
ています。

▲ 図 8

2018 年のフィッシングメール

進化するフィッシング攻撃の手法

フィッシングから人々を保護するために使用される、ツールとテクニックがより洗練されるにつれ、攻撃者は自分自身もそれに適用するように強制されます。フィッシング攻撃はますます多様化しており、単一の URL、ドメイン、IP アドレスを使ったメール送信ではなく、さまざまなインフラストラクチャーと、複数の攻撃ポイントが利用されています。攻撃そのものの性質も、数分しかアクティブでない短時間の攻撃から、期間も規模も大きな攻撃キャンペーンへと進化しています。他にシリアルバリエーション攻撃があり、この場合、攻撃者は何日か続けて少量のメールを送信し続けます。

さらに、マイクロソフトでは、攻撃者がホスト インフラストラクチャーと他のパブリック クラウド インフラストラクチャーを使用している傾向も観測しており、これは合法的なサイトやアセット間に隠れることで、検知されないようにしています。たとえば、悪意のあるペイロードや偽のログイン フォームを送信してユーザーの認証情報を盗み出すために、一般的なドキュメント共有やコラボレーション用のサイトとサービスを使用するケースがますます増えています。さらに悪意のある E メールを組織の内外に分配するために、侵害されたアカウントの使用も増加しています。

標的型から広域型まで、多様化するフィッシングキャンペーン

一般的なマルウェア分配と同様に、フィッシング キャンペーンは、標的型から広域型、汎用攻撃までさまざまです。高度に洗練された攻撃では、フィッシングしたアカウント当たりの取得金額は大きくなり、より汎用的な攻撃では、侵害したアカウント当たりの金額は少なくなりますが、広範なユーザー数をターゲットにしています。

洗練された標的型キャンペーンの例としては、[Ursnif](#) があります。この場合、攻撃者はドキュメントのファイル名をローカライズし、馴染んでいる組織または対象の業界に固有のものにします。このような攻撃は、広範なキャンペーンとはまったく異なり、より合法で信頼できるように思われます。

2018 年のいくつかの広範なキャンペーンは、ビジネス E メール危険化 (BEC) および、対象組織および洗練されたスプーフィングキャンペーン内の既知のブランド、ドメイン、またはユーザーのなりすましに関連していました。ドメイン危険化は、一般的な攻撃手法で、その E メールが信頼でき、開く必要があると組織に信じさせるものです。

多様化するフィッシング手法

マイクロソフトの研究者は、以下を含む、さまざまな種類のフィッシング手法またはペイロードが、キャンペーンで採用されていることを発見しました。

- **ドメイン スプーフィング** (E メール メッセージ ドメインは、元のドメイン名との完全一致です)
- **ドメイン危殆化** (E メール メッセージ ドメインは、元のドメイン名と類似しています)
- **ユーザー危殆化** (E メール メッセージは、信頼している誰かからのもののように見えます)
- **テキスト ルアー** (テキスト メッセージは、請求に対する正当性を伝えるために、銀行、政府機関、またはその他の会社から来たもののように表示され、通常、犠牲者にユーザー名、パスワード、または重要な金融データなどの機密情報を提供するように求めます。)
- **信用情報フィッシング リンク** (E メール メッセージに、合法的サイトのログイン ページによく似たページへのリンクが含まれているため、ユーザーはそのログイン資格情報を入力します)
- **フィッシング添付ファイル** (E メール メッセージに、犠牲者が開くように送信者がそそのかす、悪意のある添付ファイルが含まれています)

- **偽のクラウド ストレージ ロケーションへのリンク** (E メール メッセージは、正当なソースからのように表示され、ユーザーに許可を与えるか、偽のクラウドストレージの場所にアクセスする見返りに、資格情報などの個人情報を入力するようそそのかします)

攻撃者が採用する可能性のある手法はこれほど多様化しており、組織が取り組む必要があるフィッシング脅威もそれだけ複雑化することになります。

脚注

² ドメイン危殆化は、ドメインが E メール表示名として表示される例外ケースで、ドメイン スプーフィング (元のドメイン名との完全一致) と類似している可能性があります。

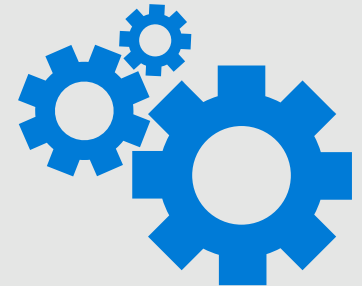
DART によるサイバー インシデント調査

大規模な製造業の組織で発生した標的型フィッシング

製造組織は、数か月のスパンで多層のフィッシング キャンペーンを体験しました。多層型フィッシングも、現在はよく見られる手法です。攻撃者は、最初のフェーズで予備調査を実行し、2 番目のフェーズで高価な資産をターゲットにします。このキャンペーンの最初のフェーズでは、組織内の小さな対象グループに送信された、メールに埋め込まれている Web ページ リンクに基づいた、よく知られているフィッシング詐欺が利用されました。メールには、ターゲットによるレビュー待ちの重要な電子ドキュメントがあるため、受信者はドメイン資格情報を使用して認証し、アクセスしてほしいというメッセージが記載されていました。この重要なドキュメントをターゲットに確認させるために偽のランディング ページが作成されました。実際はこのページで資格情報を不正取得することで、攻撃者が世界中どこにいても Office 365 アカウントにアクセスできるようになってしまいます。フィッシング キャンペーンの 2 番目のフェーズは、組織内部の機密資産を対象にした類似のフィッシング メールを送信し、より貴重なデータへのアクセスを取得しようとするものでした。マイクロソフトのお客様である同組織とマイクロソフトの連携は、この第 2 フェーズから開始されました。このインシデントからお客様が得た主な教訓は、フィッシングは最も有効な攻撃手法の 1 つであり、

リンクの最も弱い部分が「ユーザー」だということでした。ユーザーに対してフィッシング詐欺に注意するようトレーニングし、ツールを適所に配置して、攻撃者を識別して対応し、定期的にシステムのパッチを当てることがすべて重要です。組織がこれらの 1 つにも対応していない場合、脆弱になる可能性があります。

この場合、顧客の最も重要な関心事は、侵害されたアカウントへのアクセスを即座にブロックする必要がありますでした。そこで DART は、Azure Identity チームと Office 365 チームの連携に基づき、Microsoft Azure Log Analytics ソリューションを新たにデプロイし、攻撃者をネットワークから排除し、コマンド アンド コントロール チャンネルへのあらゆるトラフィックを監視する計画を立案しました。その結果、わずか 3 時間で危機的状況から脱することができました。攻撃者のアクセスが即座にブロックされたことで、被害規模の評価と回復をすぐ開始することができました。DART は、Azure Log Analytics ツールを使用して、攻撃者の行動を追跡しましたが、それによって組織の多くの構成課題が明らかになりました。例えば、DART は、重大なサーバー上のパッチ当てでギャップを識別し、インターネット上の既知の不良ホストと通信しているネットワーク上のコンピューターを検出し、マルウェア保護のないいくつかの重要なサーバーも見つけました。



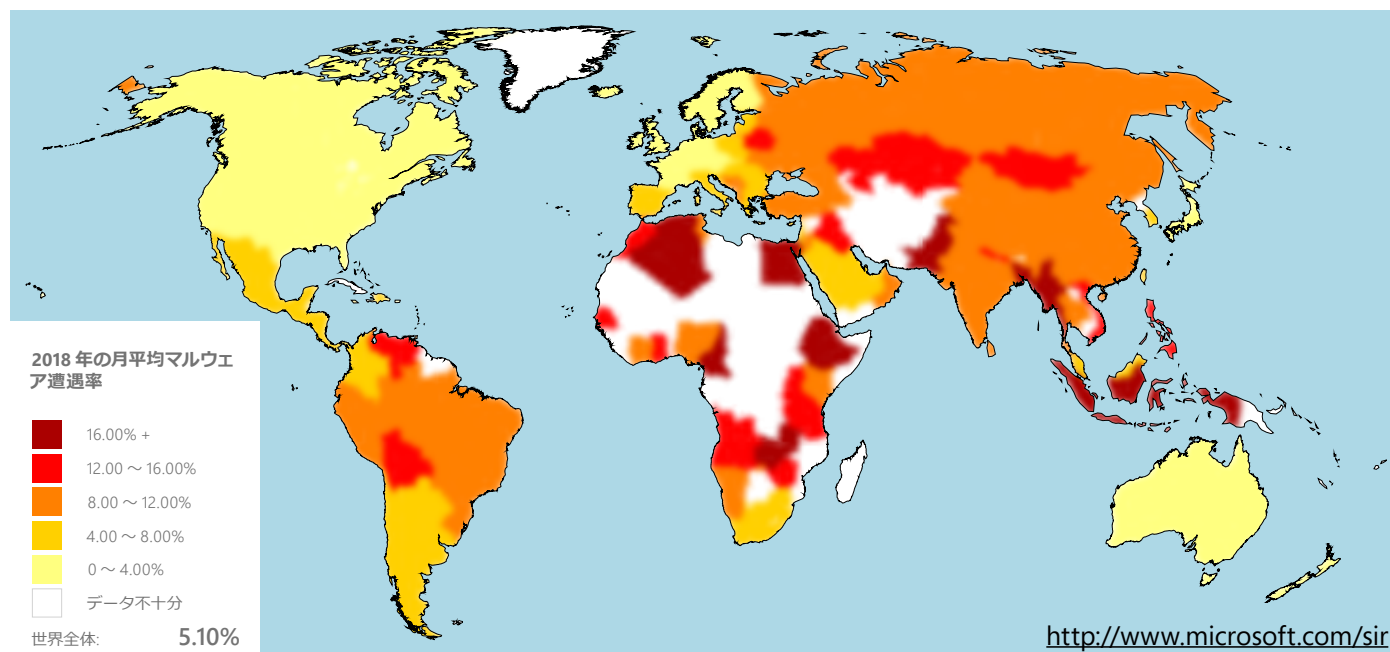
セクションⅣ

全世界の マルウェア



マルウェアは、組織と個人に、不十分なユーザビリティ、データ損失、知的財産の盗難、金銭の損失、精神的苦痛の形でリスクを課し、人の命さえも危険にさらします。マイクロソフトでは、ツールとテクニックの広範な配列を使用して、見つかったマルウェア感染を識別、ブロック、および絶滅します。

マルウェアの感染率は、2017年には5%程度から7%以上の範囲でした。2018年の初期には上昇しましたが、その後、減少して4%やや上で推移しています。**2018年のマルウェア遭遇率の全体的な減少**でいくつか考えられる理由は、Windows 10の適用の増大と、保護用のWindows Defenderの使用増大です。遭遇率とは、当該月中にマルウェアとの遭遇を報告したWindows Defender Antivirusを実行しているコンピュータの割合で、Defenderがブロックした感染試行を含みます。



◀ 図9

2018年の全世界の月平均マルウェア遭遇率
(国/地域別)

2018 年の 1 月～ 12 月中にマルウェアの遭遇率が高かった 5 つの国は、エチオピア (月平均遭遇率 26.33 %)、パキスタン (18.94)、パレスチナ領域 (17.50)、バングラデシュ (16.95)、およびインドネシア (16.59 %) で、それぞれの月平均遭遇率は、当該期間中ほぼ 16.59 % 以上でした。感染率は、社会における人材の成熟度およびテクノロジー対応状況と強く相関する傾向があります。2018 年に遭遇率が高かったすべての場所は、United Nations International Telecommunication Union (ICT) が発行した、2017 Information and Communications Technologies (ICT) Index で国と地域の下位 40 % にランクされていました。

同じ期間にマルウェアの遭遇率が低かった 5 つの場所は、アイルランド (1.26)、日本 (1.51)、フィンランド (1.74)、ノルウェー (1.79)、およびオランダ (1.82 %) で、それぞれの月平均遭遇率は、当該期間中 1.82 % 以下でした。これらの場所には、成熟したサイバーセキュリティ インフラストラクチャー、およびクリティカルなインフラストラクチャーを保護し、基本的なセキュリティに関して市民と対話するための十分に確立されたプログラムがある傾向があります。

マルウェアの影響を最も受けた国の月平均遭遇率



エチオピア: 26.33%



パキスタン: 18.94%



パレスチナ自治区: 17.50%

DART によるサイバー インシデント調査

国家支援の攻撃により業務中断を余儀なくされた、複数の金融サービス企業

DART が突き止めた破壊的インシデントで代表的なものの中から、国家支援による APT 攻撃グループに狙われた複数の金融サービス企業の事例を紹介します。この攻撃グループは前述の事例のグループとは異なりますが、実施された APT 攻撃には多くの共通点がありました。

この APT は、スパイ フィッシング E メール経由で、高度に標的を絞り難読化されたバックドア インプラントを使用し、患者ゼロ マシンに感染後、管理アクセス権を取得しました。その後、APTは複数の不正取引を実行して、大量の現金を外国銀行アカウントに送金しました。企業によっては攻撃者が 100 日以上も潜伏していたケースがありました。攻撃者は、検知されたと悟った後、即座に前段の攻撃をデブロイして、破壊的なマルウェアをその環境内の半数を超えるシステムに配信しました。これらの顧客の運営は数日間シャットダウンされました。

これらのインシデントから、顧客にはいくつかの主要な教訓がありました。まず、システムの定期的な更新 (オペレーティング システムとセキュリティの両方)、修正プログラム適用、監査などのソフトウェア ライフ サイクル管理が特に重要だということです。たとえば、非常に大規模なワークロードを実行していた Linux システム環境が完全に管理不能になり、きわめて高い攻撃リスクにさらされた組織がありました。2 番目の教訓は、主要なデータの損失に備えて、システム データのバックアップを、

オフラインの場所に保持することが重要であるということでした。もう 1 つの教訓は、敵対的アクティビティについて知る必要がある場合、従来のウイルス対策ソリューションでは不十分ということでした。

これらの組織にとって、正常な運用モードに戻ることが最優先課題でした。DART はまず最初に影響を調査し、次に影響を受けたシステムからマルウェアを除去し正常な状態に戻すことで、サービスの復元をサポートしました。さらに、EDR を始めとするマイクロソフトの脅威調査ツールの使用方法に関するトレーニングを実施して、ネットワーク内の異常動作や攻撃者の活動をお客様自身で探索できるようにしました。その中で DART は、従来のウイルス対策ソリューションが検出できない高度な標的型攻撃から防御するためには、エンドポイントの監視が欠かせないことを伝えました。



ガイダンス



ガイドンス

組織的なレジリエンスと意味のあるリスク削減を構築するには、防止、検知、応答を含むセキュリティ アプローチが必要になります。これらのカテゴリに対して、次のような推奨されるセキュリティ ベスト プラクティス、およびコントロールを編成しました。

予防:

予防的コントロールは、適切な投資によってサイバー犯罪者の攻撃コストが増大し、このように膨らんだ攻撃コストが長期に維持されるため、防御戦略全体で主要な役割を果たします (エキスパート アナリストによる出力の監視および解釈不要)。予防的コントロールの投資は、最低価格のテクニックにターゲットを絞り、安くて効果的な攻撃テクニックを着実に除去するようする必要があります。

予防に関して考慮すべき事項は次の 4 つです。

1. セキュリティ衛生は不可欠です。このレポートで共有されているいくつかのサイバー インシデントで分かるように、共通の衛生問題により、高度なセキュリティ機能の土台が壊される可能性があるため、次のようなヒントがリスクの緩和に役立ちます。

- 無料または海賊版のソフトウェアの使用を避けます。信頼できるソースからのソフトウェアのみ使用します。
- 優先管理者アカウントの確保を含む、信用情報窃盗のリスクを緩和します。その方法については、この [ブログ](#) を読んでください。ここには、マイクロソフトが自分自身のセキュリティ姿勢とイニシアティブの

計画に役立て、いくつかの規定されたロードマップをガイドおよび拡張するために使用した、いくつかの原則とツールの概要が示されています。

- ソフトウェア ベンダーから提供された安全な構成ベースラインを適用します。
- 最新の更新プログラムをオペレーティング システムとアプリケーションに適用し、OS、ブラウザ、および E メールの重要なセキュリティ更新プログラムを即座に適用することで、マシンを最新の状態に保ちます。更新またはパッチできないマシンは隔離 (または引き下げ) します。
- 高度な E メールおよびブラウザの保護を実装します。近代的なフィッシング バリエーションから防御するために、高度な脅威保護機能を持つ安全な E メールゲートウェイをデプロイします。
- ホストのマルウェア対策とネットワーク防御を有効にして、クラウドからほぼリアルタイムのブロック応答を取得します (ソリューションで利用できる場合)。

2. アクセス制御を実装します。以下のことを考慮してください。

- 最少権限の原則を適用します。この中には、ネットワーク セグメンテーションの実装、エンドユーザーからのローカル管理者権限の削除、コンピュータ上で実行されているアプリケーションに対して何らかの許可を付与する際の注意の行使が含まれています。
- ユーザーが実行できるアプリケーションを制限するなど、厳格なコード整合性ポリシーをデプロイします。
- ユーザーが実行できるアプリケーションを制限するなど、強力なコードの整合性ポリシーをデプロイします。可能であれば、システム コア (カーネル) でのコード実行を制限し、未署名のスクリプトやその他の信頼できないコードをブロックするセキュリティ ソリューションを適用します。アプリケーション ホワイトリストを使用します。
- ソフトウェア サプライ チェーン攻撃およびその攻撃を防ぐ方法については、マイクロソフト研究者のブログを参照してください。

3. バックアップを保持する。

- 重要なシステムとデータに関しては、耐破壊性のあるバックアップを作成します。
- データ オンラインの自動バックアップには、クラウド ストレージ サービスを使用します。オンプレミスのデータについては、3-2-1 ルールを使用して、重要なデータを定期的にバックアップします。データのバックアップは、3 つ保持します。2 つは異なるストレージ タイプ上に、少なくとも 1 つはバックアップ オフサイトに保持します。

4. あらゆる不審な活動に注意し、発見した場合は常に対処する。

- 従業員には、機密情報を要求する疑わしい通信に注意するよう教え、その応答方法および組織のセキュリティ オペレーション チームに即座に報告することを教えます。トレーニングは、ソーシャル エンジニアリングやスパイ フィッシング攻撃の緩和にも役立ちます。
- Web リンクをクリックする際は、注意してください。Web の閲覧では常に安全性を念頭に置きます。安全が確認されていないサイトへのアクセスに対して警告を表示するか、アクセスをブロックするソリューションを採用することで、仮想通貨マイニングとかかわりがある Web サイトとの遭遇率を削減できます。
- コンピューターの実行速度が極めて遅い場合は、実行中の疑わしいファイルを見つけ、サンプルをオペレーティング システム ベンダーに自由に送信してもらって構いません。マルウェア解析用のファイルは、マイクロソフト (<https://www.microsoft.com/wdsi/filesubmission>) に送信できます。

検知と応答:

検知と応答は、攻撃者がリソースにアクセスする時間を制限することで、レジリエンスに役立ちます。これにより、攻撃者のコストが増大し (操作を再試行または変更する必要がある)、収益が減少する (目的達成の可能性が制限される) ため、攻撃者の ROI が減少します。

事業部門の市場ニーズを満たす能力を高めるクラウド テクノロジと同じ技術を、セキュリティ運用部門の攻撃者への対抗能力の向上に活かすことができます。



◀ 図 10

SOC の進化の軌跡

Security Operations Center (SOC) の進化の軌跡を見ると、テクノロジーによって SOC の決定と対応の速度および質が継続的に増加していることが分かります。これらの革新の多くは、USAF Colonel John Boyd によって文書化された Observe Orient Decide Act (OODA) “ループ” の各段階にマップできます。³

監視 – SOC は、利用可能で広大なセキュリティ インテリジェンス (出所: マイクロソフトおよびその他のソース) にタップして、組織内および外部環境でその視野を劇的に広げることができます。

情勢判断 – これらの新しいデータ ソースが既に過負荷状態の SOC で利用可能になるため、マシン ラーニング (人工知能のサブセット) は、これらの巨大なデータセットを分別して、調べる価値がある異常を識別するための不可欠なツールになります。セキュリティ ベンダー (マイクロソフトを含む) は、イベントの優先順位付け (およびこれらの個別イベントの全体的なインシデントへの融合) のため、マシン ラーニング テクノロジーを適用しています。

意思決定 – 攻撃の分量と複雑さはすぐに SOC を過負荷状態にする可能性があるため、アナリストとインシデント応答者は、多くの意思決定を行い、アラートや検知に

対して即座に対応する必要があります。マイクロソフトとその他のベンダーは、調査機能を自動化し、ガイダンスを整備することで、迅速かつ的確なアナリストの判断 (感染や侵害の可能性があるデバイスをどのように隔離するかなど) を支援しています。当面、自動化はプライオリティの低いインシデントの解決に焦点を当てているため、特殊なスキルはより複雑な問題に適用することができます。

行動 – 応答では、多くのテクノロジーとプラットフォームにわたって迅速で正確な実行が求められ、これこそセキュリティ編成および応答自動化テクノロジーが可能にするものです。マイクロソフトおよびその他多くの企業は、近代的な脅威検知および自動応答ソリューションを含む、これらのテクノロジーに継続的に投資を続けます。

脚注

³<http://www.militaryhistoryveteran.com/colonel-john-boyd-ooda-loop/>

最先端の SOC が採用しているその他の方針をいくつか紹介します。

- **アラート フィードの量より質** – 組織が “不十分な情報” の管理から “多すぎる情報” の管理にシフトするにつれ、高度に特化した SOC アナリストがますます貴重になります。これにより、Tier 1 または Tier 2 アナリストの協力を求める警告の品質を高めることが急務となります。調査や積極的な措置の実施には追加のデータ フィードが役に立ちますが、マイクロソフトの Corporate IT SOC では、アナリストによる応答が必要なアラート フィードの真陽性率 (現時点で 90% 以上を要求) を測定しています。
- **データ グラビティ** – 巨大なデータセット (セキュリティ データを含む) の解析は、下層の未加工データに対するアクセスなしでは困難です。より多くのセキュリティ データが利用可能になるにつれ、クラウドでセキュリティ解析を実行する方が、そのデータをオンプレミス システムにバックホールするより経済的かつ実用的です。このため、ハイブリッド SIEM アプローチまたはサービスとしてのネイティブ クラウド SIEM の適用を含む、SIEM および SOC アーキテクチャの展開が有力な選択肢となります。
- **ハイ コンテキスト** – この種の検知は、データセットをより効果的に相関させられるため、はるかに役に立ちます。ネットワーク トラフィックに基づく従来の検知手法にもセキュリティ面での価値はありますが、一般的な未加工のネットワーク トラフィックには、正当な活動と異常な活動を区別するためのコン

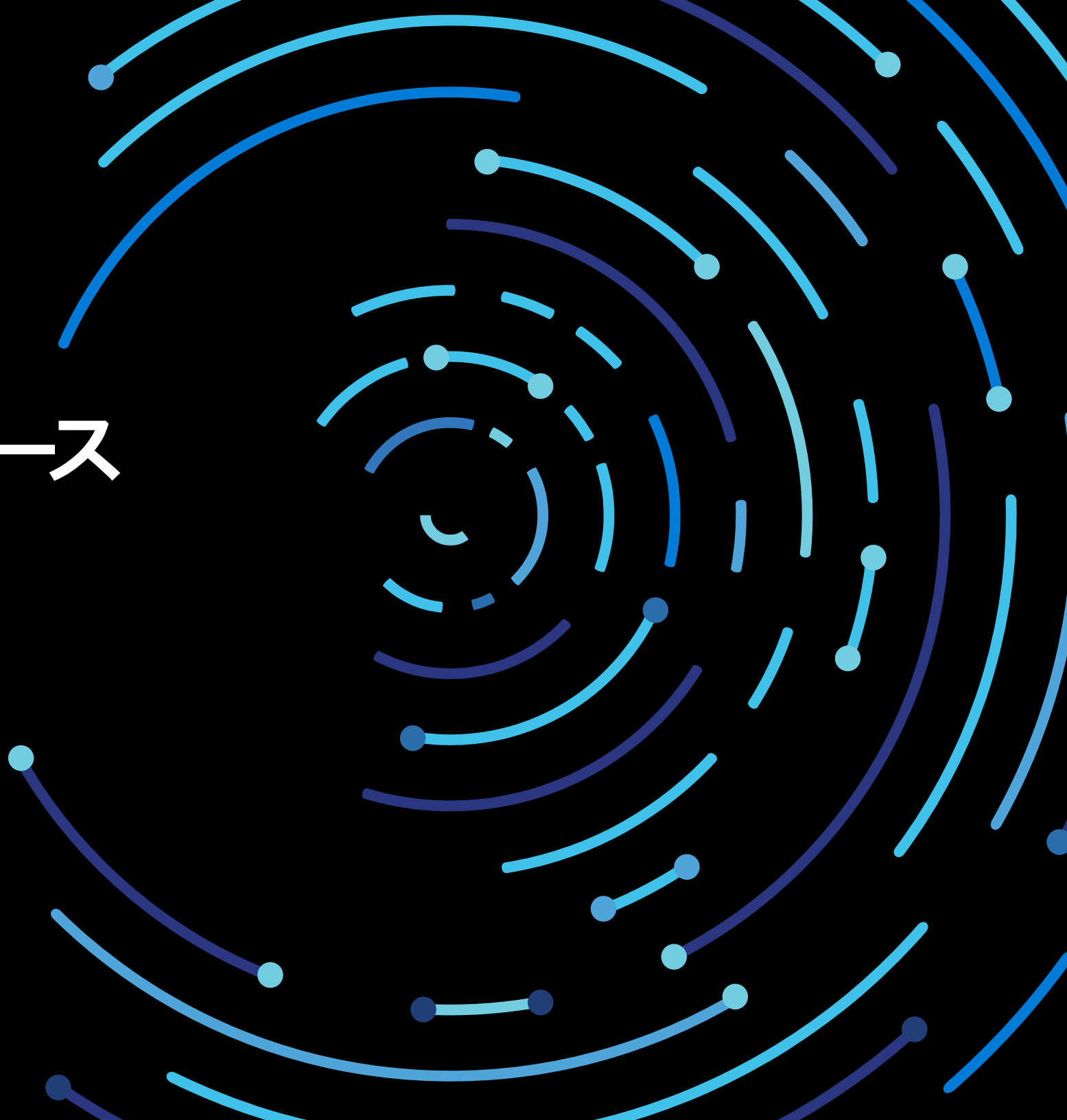
テキストはありません。マイクロソフトでは、コンテキスト情報を豊富に得られる次のような SOC による検知が、多くの価値をもたらしていることを確認しています。

- **Endpoint Detection and Response (EDR)**
ソリューション (ホスト アクティビティに関するディープ コンテキストを有するもの)
- **アイデンティティ ベースの検知**で、通常のユーザー認証パターン (場所、時間、アクセスしたサービスなど) に関するインサイトを含み、動作分析を適用するもの

技術的特性が比較的シンプルな IP トラフィックとは異なり、再現すべき操作が大幅に複雑化するため、豊富なコンテキストを入手できるこれらの検知手法は、攻撃者にとって侵入のハードルが高くなります。

顧客での大きな漏洩から学んだもう 1 つの教訓は、IT 機能を部分的または完全に外部委託している場合の、インシデントに対する迅速な対応の難しさでした。このためマイクロソフトでは、IT のアウトソーシング契約やサービスレベル契約 (SLA) を精査して、セキュリティ対応をサプライ チェーン ベンダーに任せられることを確認するよう推奨しています。顧客でのインシデント調査から学んだ内容の詳細については、<https://aka.ms/IRRG> にある [Incident Response Reference Guide \(IRRG\)](#) を参照してください。

データソース



データ ソース

マイクロソフトでは、[マイクロソフトのプライバシーに関する声明](#)で述べているように、広範なマイクロソフト製品とサービスを提供する過程で、マイクロソフト セキュリティ インテリジェンス レポートに含まれているデータを収集しました。このデータにより、当社の製品とサービスのセキュリティと操作に関する貴重な情報と、サイバーセキュリティの脅威に満ちた環境に関するインサイトが提供されます。このデータには、次のソースからの解析が含まれています。⁴

- [Azure Security Center](#) は、クラウド ワークロードのセキュリティに対する可視性を向上し、高度な分析および脅威インテリジェンスを使用して、攻撃を検知することで、組織による脅威の防止、検知、および対応を支援するサービスです。
- [Bing](#) は、悪意のあるコンテンツを見つけ出すために、年に数十億回もの Web ページ スキャンを実行する、検索および意思決定エンジンです。そのようなコンテンツを検出すると、Bing はユーザーに警告を表示して、感染の防止を支援します。
- [Exchange Online](#) は、マイクロソフトがホストしている電子メールおよび生産性サービスです。Exchange Online マルウェア対策およびスパム対策サービスは、毎年数十億のメッセージをスキャンして、迷惑メールとマルウェアを識別し、ブロックします。
- [悪意のあるソフトウェアの削除ツール \(MSRT\)](#) は、マイクロソフトが顧客のコンピューターから特定の蔓延しているマルウェアを識別して、削除するために設計した無料のツールです。MSRT は、主に Windows Update、Microsoft Update、自動更新を通じて、重要な更新プログラムとしてリリースされています。このツールのバージョンは、Microsoft ダウンロード センターからも入手できます。MSRT は、最新のリアルタイム ウイルス対策ソリューションの代替ではありません。
- [Microsoft Safety Scanner](#) は、無料でダウンロードできるセキュリティ ツールで、必要に応じてスキャンを実行し、マルウェアやその他の悪意のあるソフトウェアを駆除することができます。Microsoft Safety Scanner は、リアルタイム保護を提供せず、コンピューターの感染を防ぐことができないため、最新のウイルス対策ソリューションに代わるものではありません。

脚注

⁴重要なことですが、このデータは、プライバシーとコンプライアンスの厳密な条件を満たしてから、セキュリティのために使用してください。

- [Microsoft Security Essentials](#) は、無料で簡単にダウンロードできるリアルタイム保護製品で、Windows Vista および Windows 7 用の基本的で、効果的なウイルス対策およびスパイウェア対策保護を提供します。
- [Microsoft System Center Endpoint Protection](#) (以前の Forefront Client Security and Forefront Endpoint Protection) は、エンタープライズ デスクトップ、ラップトップ、およびサーバーのオペレーティング システムに対して、マルウェアや好ましくないソフトウェアからの保護を提供する統合された製品です。これは、Microsoft Malware Protection Engine と Microsoft ウィルス対策署名データベースを使用して、リアルタイム、スケジュール済み、およびオンデマンドの保護を提供します。
- [Office 365](#) は、組織およびホーム ユーザー向けの Microsoft Office サブスクリプション サービスです。サブスクリプション プランの選択には、Office 365 Advanced Threat Protection に対するアクセスが含まれています。
- Windows 10 の [Windows セキュリティ](#) は、マルウェアや好ましくないソフトウェアのリアルタイム スキャンおよび削除機能を提供します。さらに、Windows の最新バージョンでは、[マシン構成](#)、デバイスのパフォーマンスや健全性、その他の情報など、豊富なコンテキスト データを活用して、顧客のセキュリティを強化しています。同時に、Windows 10 では、顧客にプライバシーに関する情報をより多く提供することで、その権限を強化しています。[このブログ](#)を読んで、マイクロソフトがそのために行ういくつかの方法を学んでください。
- [Windows Defender Advanced Threat Protection](#) は、Windows 10 Anniversary Update およびそれ以降のバージョンに組み込まれたサービスで、企業顧客がネットワーク上での先進の持続的脅威やデータ漏洩を検知、調査、および修復できます。
- [Windows Defender Offline](#) は、ダウンロード可能なツールで、これを使用すると、ブート可能な CD、DVD、または USB フラッシュ ドライブを作成して、コンピューターでマルウェアやその他の脅威をスキャンできます。これは、リアルタイム保護を提供せず、最新のマルウェア対策ソリューションの代替でもありません。
- [Windows Defender SmartScreen](#) とは、Microsoft Edge と Internet Explorer の機能で、フィッシング サイトやマルウェアをホストしているサイトに対するユーザー保護を提供します。マイクロソフトでは、では、Microsoft Edge、Internet Explorer、およびその他のマイクロソフト製品およびサービスのユーザーによって報告された、フィッシングおよびマルウェア サイトのデータベースを維持しています。フィルターを有効にしているユーザーがデータベースに登録されているサイトにアクセスしようとする、ブラウザは警告を表示し、ページへのナビゲーションをブロックします。