X-Force

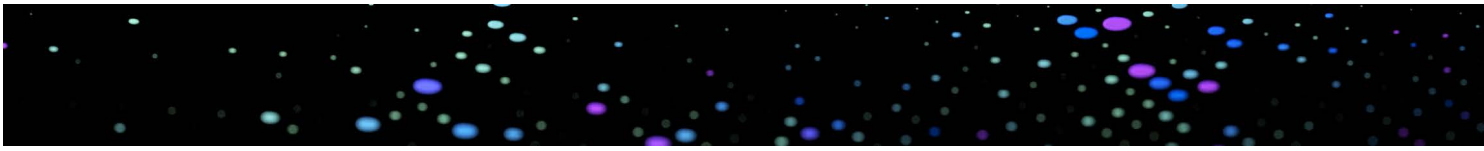
2021 IBM Security X-Force クラウドの脅威の状況に関するレポート

IBM Security X-Force 脅威インテリジェンス

スペシャル・インテリジェンス・レポート

IBM

目次



はじめに

2020 年、IBM Security X-Force はクラウド環境を標的とする脅威アクターを取り巻くグラウンドトゥルース（ground-truth）統計について、独占的な調査研究とデータを盛り込んだレポートを作成しました。クラウドはオンプレミスのインフラよりも利便性と経済性に優れ、ほぼ永続的なアップタイムが得られることから、企業への積極的な導入が続いています。

同時に、脅威アクターが組織規模を問わずクラウド環境を標的としている状況にも変化はありません。そのためクラウド・モデルに移行するには、従来型の展開とは異なる、特別なアプローチが必要です。クラウド環境の展開、そして管理を成功させるには、脅威アクターがいかにしてクラウドを標的とするのか、その動機は何か、そしてどうすればクラウドを脆弱にするありがちなミスを回避できるかを理解することが重要な鍵となります。

今年、私たちは 2020 年のレポートに 2020 年第 2 四半期から 2021 年第 2 四半期までのデータを新たに追加し、内容の充実を図りました。このレポートにはダーク・ウェブの分析、IBM Security X-Force Red ペネトレーション・テストのデータ、IBM Security Services のメトリック、X-Force Incident Response の分析、X-Force 脅威インテリジェンスの調査などのデータ・セットを使用しましたが、私たちはこのような複数のデータ・ソースを駆使して、脅威アクターがどのようにしてクラウド環境に侵入し、侵入後にどういったタイプの悪意ある活動を行っているのか、そしてどうすればクラウド環境に関わるセキュリティー・インシデントに効果的に備え、対応できるのかを、さらに深く理解することができました。

要点

クラウド環境ではセキュリティーを強化する必要がある

ダーク・ウェブに存在するクラウドのアカウント/リソース: ダーク・ウェブにはパブリッククラウドへのアクセスを売買する活発な市場が存在し、そこで行われる何万件ものクラウド・アカウントやリソースの販売が喧伝されています。

—事例のうちの 71% で、脅威アクターは Remote Desktop Protocol (RDP) アクセスを提供し、攻撃者がクラウド・リソースに直接アクセスして悪意ある活動を行えるようにしていました。

—クラウド環境にアクセスするためのアカウントの資格情報が数ドルで売られているケースもありました。

パスワードとポリシー: X-Force Red によるクラウド環境のペネトレーション・テストでは、その大部分でパスワードかポリシーのいずれかに問題があることが判明しています。

システムの強化: X-Force の調査によれば、クラウド環境への侵害の 2/3 は、セキュリティー・ポリシーの適切な実施やシステムへのパッチの適用といった、より堅固なシステムにすることで防止できた可能性があります。

クラウド展開アプリケーションの脆弱性の急増: クラウド展開アプリケーションでは、今日に至るまで 2,500 を超える脆弱性が判明していますが、そのうち約半数は過去 18 カ月間に明らかになったものです。この急激な増加は、一部には 2020 年 1 月に クラウドの脆弱性が MITRE の CVE 基準に追加され、追跡が進んだことによるものと考えられます。その一方で、無防備な脆弱性が増えたことに伴うリスクの増大にきめ細かく対処することが肝要であることも鮮明になりました。

要点

脅威アクターは弱点を狙う

パブリック API のポリシーが大きなセキュリティー・ギャップをもたらしています。被害のあったお客様のデータを X-Force Incident Response が分析した結果によれば、アプリケーション・プログラミング・インターフェース（API）の不適切な構成に絡むインシデントは 2/3 に上ります。

クラウドを標的とした攻撃ベクトルのうち、X-Force が観測した中で特に多かったのは、**オンプレミス環境からクラウド環境にピボット**する脅威アクターでした。このような横展開は、2020 年に X-Force が対応したインシデントのほぼ 1/4 で見受けられました。

IBM の推定によると、クラウド環境に対する侵害の半数以上は「**シャドー IT**」が原因で発生しています。シャドー IT は正式に許可されていないシステムがセキュリティー・ポリシーに反して運用されて生じるもので、多くの場合、脆弱性やリスクのアセスメントも、セキュリティー・プロトコルの強化も不十分です。

脅威アクターは、クラウドに狙いを定めた攻撃に引き続き投資している

データの分析結果によれば、クラウド環境に送り込まれるマルウェアで最も多いのは依然として**クリプトマイナーとランサムウェア**で、これらは検知されたシステム侵入の半数以上を占めています。

クラウドを標的とするマルウェア開発は続いており、Docker コンテナにフォーカスした古いマルウェアの新しい亜種に加え、クロスプラットフォームで動作する Golang のようなプログラミング言語で書かれた新しいマルウェアも登場しています。

ダーク・ウェブ市場で活発に取引されるクラウド・アクセス

IBM はダーク・ウェブやディープ・ウェブにおけるクラウド・アカウントへのアクセスの販売状況を調査しましたが、その結果はまさに戦慄すべきものでした。数万件のアカウントとリソースが、複数のダーク・ウェブ市場で売買されている可能性が明らかとなったのです。その圧倒的多数は自動的にダーク・ウェブ市場に投入されていました。多様な情報窃盗ツールやマルウェアが隙を狙って被害者のシステムに侵入し、売買の対象となる資格情報を出品していたのでした。クラウド・リソースへの侵入が多数発生しているという事実は、これらのプラットフォームが脅威アクターにとって悪意あるさまざまな目的に非常に利用しやすいものであることを浮き彫りにしています。

以下は IBM のダーク・ウェブの調査に基づく分析です。このような調査の内容はその性質上、常に変化していますが、これらのデータ・ポイントは、IBM が 2020 年 7 月から 2021 年 7 月にかけて複数のダーク・ウェブ市場を調査した結果得られた、代表的な知見となります。

IBM の調査から、一部のクラウド・アカウントが他のアカウントより高く取り引きされていることが判明しました。これから紹介するデータは、企業が自社のクラウド環境がサイバー犯罪者にとってどれほど価値があるかを理解し、彼らから攻撃される可能性を推定して、より的確にリスクを評価するのに役立ちます。

販売されるクラウド・アカウントはピンからキリまで

前述の期間中にダーク・ウェブ市場で販売されていた可能性のあるクラウド・アカウントは、X-Force の調査で 30,000 件近くに上りました。脅威アクターは、さまざまなコモディティーあるいはオープンソースの情報窃盗ツール、マルウェア使用し、入手したクラウド・アカウントの大多数の情報をリストにして市場に投入します。そのためこの活動を支えるアクターの数を見極めることは困難です。

ボットネット市場の外にある、ダーク・ウェブの他のフォーラムに掲載された広告では、1 件のアカウント・アクセスの資格情報に、各種の条件に応じて数ドルから 1 万 5,000 ドル以上の売値が設定されていました。販売されているアカウントの価値を左右するのは、アカウントのクレジット額、地域、そのアカウントが持つ所属組織へのアクセス・レベル（root アクセスかそれより下の特権ユーザーか）などの因子と考えられます。

クラウドのクレジットを探す

クラウドに関連したダーク・ウェブ上の広告の中には、クレジットにアクセスできるクラウド・アカウントの販売に関するものも多数ありました。クラウド・アカウントのクレジットとは、そのアカウントに関連付けられている金銭的な価値であり、これを使用すればクラウド事業者からコンピューティング・リソースを追加購入することができます。例えば、ある企業があるクラウド事業者のクラウド・アカウントを持っていてこのアカウントに 1,000 ドル分のクレジットを購入している場合、そのアカウントを入手できれば自由にリソースを拡張できてしまいます。

クレジット額に応じて、15 ドルから 30 ドルごとに、クラウド・アクセスの価格は平均で 1 ドルずつ上昇していました。利用可能なクレジットが 5,000 ドルであれば、そのアカウントの価値は約 250 ドル（比率が 20:1）ということになります。アカウント・アクセスのこのような料金体系には銀行口座に不正アクセスできるアクセス権の売買に類似しており、こちらもやはり口座の預金額が高いほど価格が上がります。

脅威アクターは、流出したアカウントをそのアカウントが持つクレジットの何分の一かで購入し、攻撃のホストに使用することができます。これには二重のメリットがあります。つまり、コストを削減できるうえ、ブラックリストに含まれていたり、ブロックされていたりする可能性が低い正規のリソースで、悪意ある活動ができるのです。

アクセスのコストは低く、インパクトのポテンシャルは高く

クレジット額は高くてもクラウド・アカウントの価格が低い場合、いくつかの原因が考えられます。ダーク・ウェブ市場のエコシステムに大量のクラウド・アカウントが出回っているか、逆にクラウド・アカウントの需要が少ないのかもしれません。あるいは払い戻したアカウントの現金化率が低いため、それに合わせてアカウントの価値が下がったことも考えられます。クラウド事業者や被害者がアカウントに侵入されたことに気付き、そのアカウントへのアクセスを制限したときに購入者が負うリスクも、売価が低くなる原因の 1 つに数えることができます。さらに、ある程度の額のクレジットでアカウントを簡単に開設できるため、アカウントを入手する手間と価値とが見合わないケースもあります。面白いことに、脅威アクターは販売するアクセスに保証を付けることがしばしばあり、そこでは販売から 7 日または 14 日後にアクセスが利用できなくなった場合の返金を約束していますが、これはアクセスの存続期間が長くないことを示唆しています。

盗まれたアカウントは、クラウド環境から攻撃を開始し、それを拡大するためだけなく、攻撃者がネットワークの他の部分やより多くの特権を持つユーザーへと横展開するための、組織の環境全体への足掛かりにも使われます。そのため、組織はこのような横展開の試みを、適切なファイアウォール、プロキシー、セグメンテーション、フィルタリングのメカニズムを使って阻止しなければなりません。

> 盗まれたアカウントはクラウドで攻撃を仕掛けるチャンスを敵対者に与えるだけでなく、彼らがネットワークの他の部分にアクセスするための、組織の環境全体への足掛かりにも使われます。

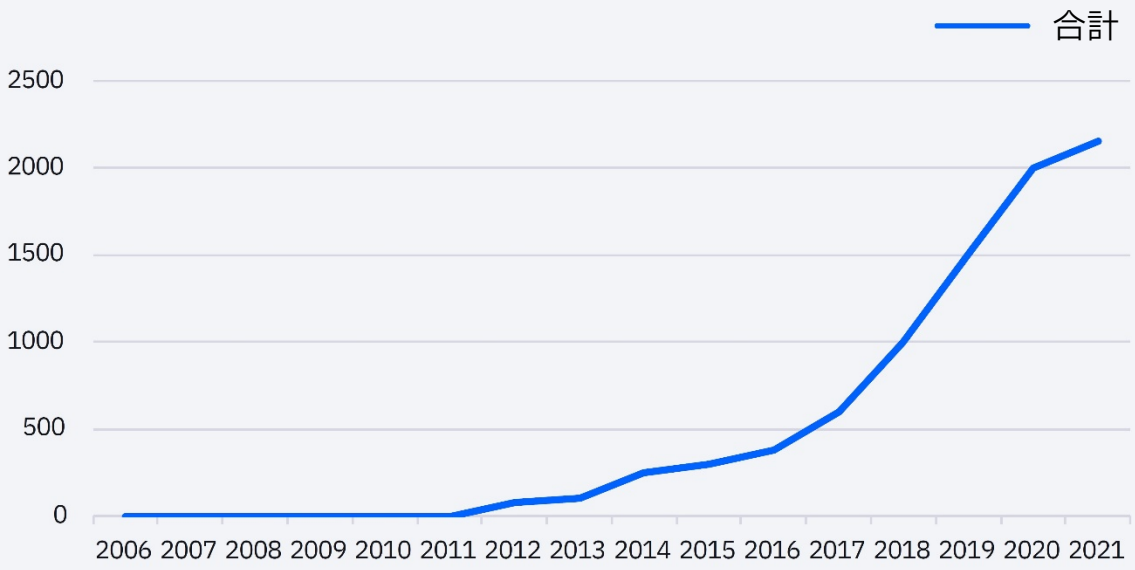
脅威アクターから見た自社の価値を評価する

ダーク・ウェブの調査からは、脅威アクターが引き続きクラウド・アカウントへのアクセスとその活用に関心を持っていることがわかります。ただし、攻撃者にとってすべてのアカウントが同じ価値をもたらすわけではなく、何らかの要素が組織のアカウントの価値を高める場合があることも IBM の調査で明らかになっています。例えば、多額のクレジットを保有する西ヨーロッパのアカウントは脅威アクターにとって極めて価値が高いと考えられ、組織の脅威プロファイルもおそらく大きくなるはずです。そのようなアカウントはサイバー犯罪者からの人気が高く、短期間で売れることは間違いありません。

クラウド環境の脆弱性の増加と深刻化

クラウド環境には数え切れないほどのセキュリティー上の利点がありますが、その一方で、攻撃者がクラウド環境への侵入に利用できる新たな脆弱性が研究者たちによって次々と発見されています。IBM の調査によれば、クラウドに展開されているアプリケーションの脆弱性は増加の一途を辿っており、現在ではその総数は 2,500 超、この 5 年間で 150% の増加となっています。

クラウドに展開されているアプリケーションの脆弱性の数（X-Force 調査）



脆弱性に関しては、IBM Security X-Force Red が多面的なランキングのアルゴリズムを用い、脆弱性の深刻度を「リスク・スコア」で採点しています。リスク・スコアは、使いやすさ、許可されるアクセス・レベル、被害を受けた場合のシステムへのインパクトといった多様な因子を使用して、脆弱性を正確に測定します。

X-Force Red のデータによれば、クラウドを標的とした脆弱性の深刻度は近年大幅に増しています。これは、組織が重要なデータをマルチクラウド環境を利用して保存するケースが増えていることを脅威アクターが把握しているためと考えられます。クラウド環境は交通量の多いデータ・ハイウェイであり、脅威アクターにとっては標的に事欠かない、魅力的な攻撃対象領域なのです。

クラウド環境への脅威アクターの侵入方法

脅威アクターによるクラウド・データへの不正アクセスは続いています。IBM は彼らの企業のクラウド資産を狙う手口への理解を深めるため、今年のレポートに新たなデータ・ポイントを多数盛り込みました。

150%

クラウドの脆弱性は増加傾向にあり、この 5 年間で 150% 増加しています。

パスワードやポリシーの違反はシャドー IT が原因となっているケースが少なくなく、これがクラウド環境にとって引き続き悩みの種となっています。X-Force Red が 2021 年に実施したクラウド環境のペネトレーション・テストでは、その大多数において 2 つの要素のうち少なくとも 1 つに問題があることが判明しました。この 2 つの要素は、組織で特によく見られる初期感染のベクトルである資産の不適切な設定、パスワード・スプレー攻撃、オンプレミスのインフラストラクチャーからのピボットなどに細分化されます。脅威アクターがクラウド環境のセキュリティーの甘さを突く手口としては、この他にも API の設定とセキュリティーに関する問題、リモート・エクスプロイト、機密データへのアクセスなどがよく使用されています。

IBM Security X-Force Incident Response の知見

IBM Security X-Force Incident Response (IR) チームは、クラウド環境の侵害に関わる過去 1 年間の事例を分析し、最も頻繁に悪用される脆弱性や設定ミスを特定しました。

— バーチャル・マシンやその他のリソースをデフォルトのセキュリティー設定のまま誤ってインターネットに公開する。プラットフォームの設定ミスとネットワーク制御の不備により、Microsoft プラットフォームの RDP (Remote Desktop Protocol) などで内部サービスを直接インターネットに公開してしまうケースがこれに該当します。他にも、部外秘のデータを保持するオブジェクト・データ・ストアが外部からアクセス可能になっていたケースがあります。

— インターネットからランディング・ページ経由でアクセスできる SaaS ソリューションやフェデレーテッド・サービスなどで多要素認証 (MFA) が行なわれていないなど、アクセス制御メカニズムが不十分。この場合、盗まれた資格情報のセットがあれば、攻撃者はアカウントの認証を一気に突破できてしまいます。

— オンプレミス環境とクラウド・コンピューティング環境との間で、仮想ネットワークのセグメンテーションの不備や信頼関係の乱れが存在する。つまり、クラウドへの侵入が、基盤となるシステム内への横展開へとつながる恐れがあるということです。

X-Force IR は、間接的にクラウド・コンピューティング環境への侵入につながる、組織面の課題も割り出しています。

— クラウド上の**脅威を監視および検知する**方法がまだ企業の間に定着していない。セキュリティー・ポリシーがクラウドに対応していなかったり、クラウド環境に応用できるインシデント対応スキルが足りなかったりすると、事態は悪化します。

— クラウド環境にセキュリティー制御を設定する際に、オンプレミス環境と同レベルの**信頼性と専門性**を実現できていない。

リソースの不適切な設定

パブリック API は広く普及しており、それを使用することによって外部ツールがクラウドの機能とやり取りし、データへのアクセスも可能になります。その結果、セキュリティーが確保されていないパブリック API の問題が随所に現れるようになりました。データのサンプルに含まれるクラウドのインシデントの 2/3 は、API キーの設定ミスによって不適切なアクセスが可能になったことに関連しています。同様に、X-Force IR チームの調査によれば、昨年はパブリック・コード・リポジトリーから API 資格情報が漏えいしたことによるクラウド環境への脅威アクターのアクセスが多発しました。

> パスワード・スプレー攻撃、ソフトウェアの脆弱性の悪用、クラウド展開時の設定ミスは、脅威アクターがクラウド環境にアクセスするのに最も頻繁に利用する方法です。

X-Force IR が調査したクラウド・ベースの侵害では、オブジェクト・ストレージ・サービスの設定ミスなどにより、セキュリティー保護されていないリソースが意図せずにインターネットに公開されたことが主な原因であった事例が多数ありました。このデータは、X-Force の研究者が観測した侵害のうち、強化策の不備に起因するものが 2/3 近くに上ったことでも裏付けられています。IBM は、分析したインシデントの過半数にシャドー IT の使用が絡んでいると推定しています。

X-Force IR が調査した事例の中で、脅威アクターがクラウド環境に侵入する手法として最もよく見られたのは、パスワード・スプレー攻撃、ソフトウェアの脆弱性、オンプレミスへの侵入からクラウドへのピボットの 3 つでした。

パスワード・スプレー攻撃

この種の攻撃は自動化が容易であり、しかも規模を拡大して一度に多くの組織を標的にすることができます。X-Force IR は、パスワード・スプレー攻撃を仕掛けられた後、不適切なアクセス制御が原因で侵入が広がってしまったケースを少なからず把握しています。推測/漏えいしたパスワードを攻撃者に使用されると、その影響はそのユーザーの特権レベルに正比例して拡大します。

ソフトウェアの脆弱性

X-Force IR のデータによれば、クラウド環境でホストされているソフトウェアの脆弱性が、攻撃者にとっての組織の環境への最初の足掛かりとなったケースは珍しくありません。クラウド対応のソフトウェアには多数の種類とブランドがあり、サイバーセキュリティーを担当するチームにとって各インスタンスのセキュリティーを個別に確保するのは困難です。そしてそれが問題を深刻化させています。

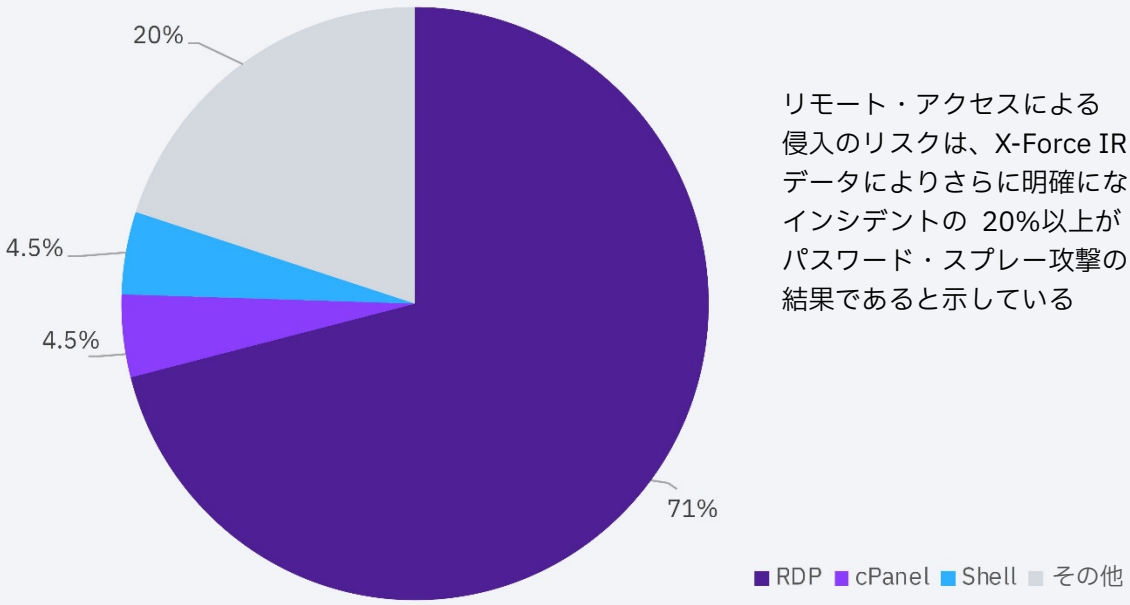
オンプレミスからクラウドへのピボット

X-Force IR が特定した上位 3 つの感染経路の最後の 1 つが、脅威アクターがエンドユーザーやオンプレミスでホストされているシステムに侵入し、そこからクラウド環境にピボットするケースです。この種の侵入はインシデント対応の 23% 以上で発生し、脅威アクターはこれを利用することによって組織への支配を強め、さらに多くの組織リソースへの侵入を可能にします。

RDP を好むリモート・エクスプロイト

ダーク・ウェブのデータは、リモート・アクセスによる侵入の有効性が高いことを裏付けています。IBM がダーク・ウェブ市場を分析したところ、ダーク・ウェブで販売されているクラウド・リソースのうち、RDP がアクセス・ベクトルとなっているものが 70% を超えることが判明しました。市場では cPanel と Shell のアクセスがそれぞれ約 4.5% のシェアを占めており、RDP のアクセスが他のアクセス方法の頻度を大きく上回っていることが推測されます。

アクセス・タイプによるダーク・ウェブのアカウント



リモート・アクセスによる侵入のリスクは、X-Force IR データによりさらに明確になり、インシデントの 20%以上がパスワード・スプレー攻撃の結果であると示している

脅威アクターからマイナー、ランサムウェア、ボットネットに利用されるクラウド環境

X-Force は IBM の IR チームのデータを分析し、侵入した脅威アクターがクラウド環境をどのように使用しているかを調べました。インシデントの分析によれば、クリプトマイナーとランサムウェアが広く使用されており、システム侵入の半数以上を占めています。クラウド環境はリソースと処理能力の拡張が可能であるため、リソースを大量に消費するクリプトマイナーにとっては魅力的な標的です。また、クラウド環境ではオンプレミスのサーバーと同レベルの監視が行われていない場合があり、そのことが脅威アクターを惹き付けるだけでなく、他のテナントへの影響が大きい DDoS ボットやクリプトマイナーなどのマルウェアが検知されないまま、長期間放置されるという事態を招きやすくしています。

クラウドでは攻撃者が攻撃規模を拡大したり、痕跡を消したりすることが可能です。しかもクラウド環境に侵入すれば、それが無料でできてしまいます。

Docker にフォーカスするマルウェア

X-Force IR は、クラウド環境に影響を与えるマルウェアのトレンドを分析した結果、マルウェアの複数のファミリーが、汎用的な Linux システムから Docker コンテナへと攻撃対象をシフトしていることを発見しました。この Docker への攻撃はレジストリーへの攻撃、ホストへの攻撃、実行中のコンテナへの攻撃の 3 つに大別できます。

XoRDDOS、Groundhog、Tsunami などのマルウェアのファミリーではこのようなシフトが顕著です。Docker に焦点を合わせたこの行動は、ボットはもとより、IoT マルウェア (Kaiji)、クリプトマイナー (Xanthe、Kinsing)、その他のマルウェア株による悪意ある活動にまで拡大しています。

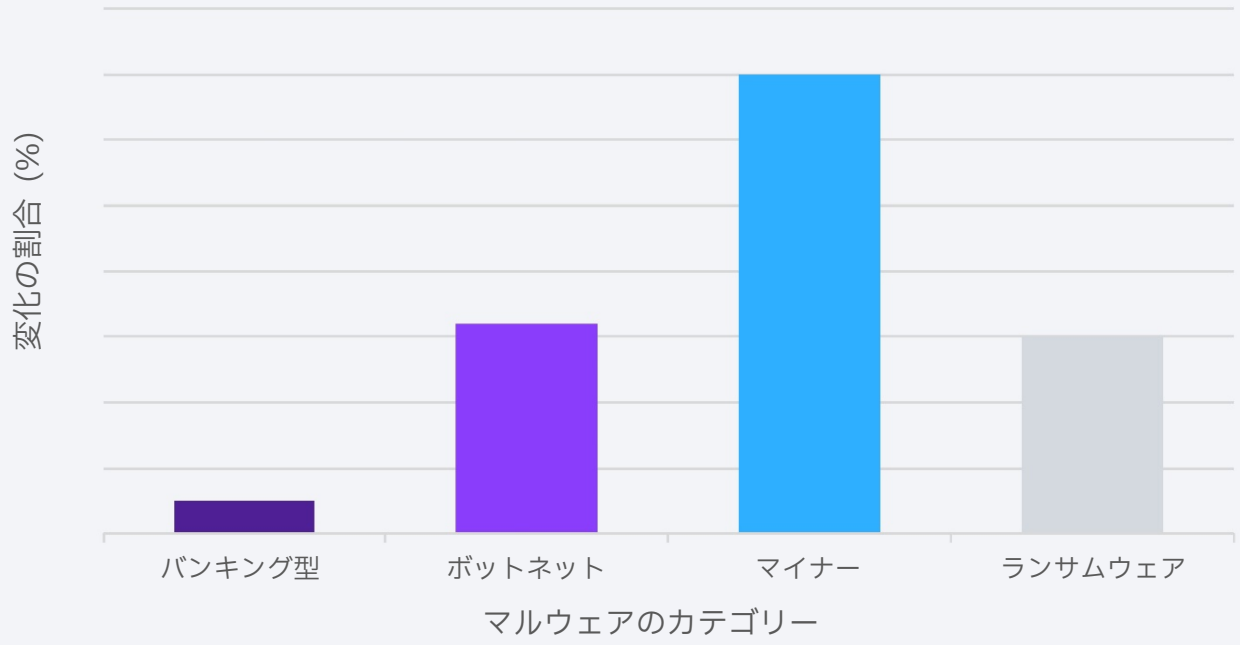
今年はボットネット・マルウェアでもクラウド環境をターゲットとするものが増えました。特に、無防備な Docker サーバーは引き続きボットネット・マルウェアの最大の標的となっているようです。Docker 以外のコンテナ・プラットフォームをターゲットとする脅威アクターも確認されています。例えば、脆弱な Windows コンテナに侵入するマルウェアの Siloscape が発見されたほか、オープンソースのコンテナ管理プラットフォームである Kubernetes も、TeamTNT などのアクターのターゲットとなりつつあります。

クラウドに主眼を置くマルウェア開発の増加

Intezer の調査では、脅威アクターがクリプトマイナー、ボットネット、ランサムウェアのコードを進化させるための投資を継続していることが明らかになりました。一方、バンキング型トロイの木馬については、脅威アクターはコードを更新するつもりはないようです。これらの調査結果は、クラウド環境が特にクリプトマイニング・マルウェアのターゲットとなりやすく、ランサムウェアやボットネットも引き続きよく見られるという IBM のデータと整合しています。

以下のグラフは、Intezer の調査に基づき、過去 1 年間に行われたマルウェアのアップデートや改変に対する投資のレベルをカテゴリー別に示したものです。変化の割合が高いのはマイナーで、使用されているコードの 7% 近くが前年とは異なっており、アクターが多大な投資を行っていることがわかります。一方バンキング型トロイの木馬の変更コードの割合は低く、1% に達しません。

ユニーク・コード文字列の変化の割合



クリプトマイナー

クリプトマイナー感染は、侵入されたクラウド環境で使用される主なマルウェアとして「2020 クラウドの脅威の状況に関するレポート」でも取り上げましたが、依然として脅威アクターが目指す最大の目標となっています。Intezer の調査によれば、クラウド環境をクリプトマイナーに感染させる方法の 1 つとして悪意のある Docker イメージが使われています。TeamTNT などの脅威アクターは、マルウェアを含むイメージを作成し、Docker デーモンへのアクセスが可能になると、そのイメージを使用して悪意あるイメージを持つ新しいコンテナを起動します。

コマンド & コントロールのシフト

脅威アクターは引き続きクラウド・インフラストラクチャーを使用して、悪意のあるペイロードをホストし、自らのオペレーションに使用するコマンド & コントロール（C2）バックエンドを確保しています。この活動については昨年のレポートでも報告しましたが、そのトレンドは拡大しており、2021 年にはさらに多くのクラウド・ベースのサービスや Web サービスが新たな検知回避策に利用されています。以下はその例です。

— クラウドを利用するバックドアに PowerSlack というものがありますが、これは人気のチャット・ソフトウェアである Slack を C2 通信に利用しています。

— Astaroth という名で知られるマルウェアのファミリーは、YouTube の動画の説明文に C2 の情報を保存し、疑わしいネットワーク・トラフィックを合法的な活動のように見せかけている可能性があります。

ファイルレス・マルウェア

メモリー内に潜んで正体を現さないファイルレス・マルウェアは、標準的な検知ツールから巧妙に逃れることができ、セキュリティー・チームもその存在に気付きません。ファイルレス・マルウェアはスクリプトで起動できるほか、現在では Golang で記述されたオープンソースのクリプター/メモリー・ローダーである Ezuri を使用することにより、検知されていないマルウェアをより簡単に起動することが可能となっています。Golang はポピュラーな言語の 1 つで、多くのクラウドネイティブ・オペレーションや攻撃フレームワークに急速に使われるようになりつつあります。

> クラウド・プラットフォームでは攻撃者が攻撃規模を拡大したり、痕跡を消したりすることが可能です。しかもクラウド環境に侵入すれば、それが無料でできてしまいます。

クラウド侵害に備え、対処するための推奨事項とベスト・プラクティス

IBM Security X-Force では、クラウド・ユーザーがクラウド・セキュリティーのインシデントに備え、対処するには、多面的なセキュリティーのアプローチの導入を検討すべきと考えています。

準備

— できる限りオープンで統合されたセキュリティーのアプローチを使用し、それによって断片化されたクラウド環境に散在するセキュリティー・データを包括的に管理できるようにします。オープン・テクノロジーを利用し、ツール間の緊密な統合を可能にする、Cloud Pak for Security などのセキュリティー・プラットフォームを検討してください。

— 仮想ネットワークのセグメンテーションを実施し、リソースへのアクセス制限や侵入発生時の横展開のリスクの削減を図るなど、ゼロトラストの指針の導入を検討します。

— セキュリティー戦略の重要な要素として、オンプレミス環境とクラウド環境の間の信頼関係を評価します。他のオンプレミスの資産と定期的にやり取りする可能性のあるプライベートクラウドでは、これは特に重要です。

— 監視および検知機能をクラウド環境に拡張します。クラウド環境の監査ログの要件を決めてそれらを実施し、クラウド・ネイティブなツールやテクノロジーを活用して、悪意あるアクティビティーや侵入の証拠を監視します。

- 要塞ホストを展開して、インターネットをはじめとする信頼度の低い、または信頼できない外部ネットワークからプライベートクラウドのネットワーク・ゾーンを隔離することにより、クラウドの攻撃対象を減らすと同時に、クラウド・リソースへの不正アクセスのリスクを最小限に抑えます。ファイアウォールやロード・バランサーは、クラウド環境に関連するゲートのトラフィックをフィルタリングするのに有効です。

- クラウド Web アプリケーションの防御策、例えば Web アプリケーションのファイアウォールや、アプリケーションおよび管理されていないクラウド・リソースの脆弱性管理などのコントロールなどを導入します。

- クラウド ID に対する最小特権の原則、特権アカウントに対する MFA、フェデレーテッド・サービス経由のクラウド・リソースへのアカウント・アクセスなどの、強力なアクセス制御のプラクティスを導入して実施します。
    - システムがポリシーを遵守しているかを定期的にテストします。
    - セキュリティー・グループの特権と新規ユーザーの作成を自動化し、最小特権をデフォルトにします。
    - IAM (Identity and Access Management) をモダナイズしてユーザー名とパスワードの組み合わせへの依存度を減らし、脅威アクターによる資格情報の盗難に対抗します。

- 強化されたコンテナ・プラットフォームを利用して、複数の環境を一貫したレベルのセキュリティーとコントロールで保護し、それらの環境上でワークロードを実行します。

- プロビジョニング・ポリシーを導入し、リソースをプロビジョニングできるユーザーとそのタイプ、期間、それらのリソースの配置など、展開するリソースのライフサイクルを管理するためのルールを実施します。
    - このコントロールは、クラウド環境が外部の脅威にさらされるリスクを減らすのに必要です。
    - 積極的に自動化を使用し、ヒューマン・エラーをできるだけ排除します。

- コンプライアンスおよびセキュリティー・ポスチャー実施ツールを使用して、クラウドのオブジェクト・ストレージのバケットがインターネットに公開されたままになっているなどの、よくある設定ミスを防ぎます。

- ペネトレーション・テストのプロジェクトを計画し、クラウドでホストされているアプリケーションや環境の脆弱性を割り出します。

- クラウド・ベースのシナリオで敵対者のシミュレーション演習を実施し、クラウド・ベースの効果的なインシデント対応の訓練を行います。

対応

- AI と自動化を推し進めインシデント対応やマルウェア分析を実行します。これによってクラウド環境に関連する侵害の対応時間や全体的な平均コストを削減できます。

- 被害を受けたマシンは再イメージングではなく再展開して、調査中のフォレンジック・アーティファクトを保存します。これによって侵害がどのように発生したのか、また、もしあるとすれば、脅威アクターが組織の環境で他に何をしたのかを後から調査することができます。

- インシデント対応に脅威インテリジェンスを活用し、脅威アクターに関する知識を生かして対応時間を短縮するとともに、より徹底した対応活動を可能にします。

- クラウド侵害への対応に適したツールと人材を組織が確保していることと、クラウド・ベースの侵害に特化したインシデント対応のプレイブックが用意されていることを確認します。

- 短縮ダイヤルにサージ支援を登録しておきます。大規模なセキュリティー・チームであっても、インシデント対応（IR）サイクルの初期段階や修復作業中にはしばしば支援が必要になります。X-Force Incident Response Retainer を導入すれば、攻撃時に必要な支援を受けるまでの時間を最小限に抑えることができます。

IBM Security X-Force について

X-Force チームには、オンプレミス、クラウド、ハイブリッドの各クラウド環境に対する侵入の調査経験を積み、業界屈指の高度なスキルを備えたインシデント対応の専門家が揃っています。また、X-Force は成熟度評価、IR プラン/プレイブックの作成、研修やシミュレーション演習などの事前対応型のクラウド・サービス・オファリングも提供しています。これらはいずれも、IBM のテレメトリーから得られた知見に基づく、業界最高レベルの X-Force 脅威インテリジェンスを基盤としています。このアプローチによって、組織ではセキュリティー・インシデントへのより効率的かつ効果的な準備、検知、対応が可能になり、また、セキュリティー・インシデントに伴う収益の損失や復旧のコストを最小限に抑えられるようになります。X-Force レポートの内容や、X-Force のサービスについて詳しく知りたい場合は、こちらからコンサルティングをご予約ください。

協力者

チャールズ・デベック

リチャード・エマーソン

アンドリュー・ゴレッキ

シャーロット・ハモンド

Intezer

スコット・ローア

ミッチ・メイン

スコット・ムーア

ジェイソン・リッグス

オスカー・サンチェス

ジョニー・シャイエブ

IBM Security

IBM Security
New Orchard Rd
Armonk, NY 10504
U.S.A.

Produced in the United States of America

IBM