X-Force

クラウドの脅威 セキュリティー・レポート 2020

IBM Security X-Force® Incident Response and Intelligence Services (IRIS)

特別インテリジェンス・レポート 2020 年第 2 四半期

IBM Security

目次

概要

運用の拡大と迅速化のためにクラウド環境を利用する組織がますます増えています。そのため、この分野で特有のサイバー脅威の状況について理解することが重要です。IBM ではそのグローバル・プレゼンスを活用して、この分野での重大な脅威を識別するために、過去 1 年間にチームが対応したクラウド関連のサイバーセキュリティー・インシデントの詳細な分析を行いました。このレポートでは、以下について、IBM Security がクラウド防御の最前線で観察していることを詳しく説明します。

— クラウド・システムをターゲットにする攻撃者

— 脅威アクターがクラウド環境にアクセスする方法

— 脅威アクターがクラウド環境に侵入した後の行動

— クラウド・セキュリティーで一般的に観察される欠陥

— 組織のクラウド・セキュリティー体制を改善するための推奨事項

主な調査結果

2019 年以降収集されている IBM Security インシデント対応データによると、脅威アクターがクラウド環境をターゲットとする最も一般的な動機は、**金銭的利益**です。[1]

45%

クラウド・アプリケーションのブルートフォースとエクスプロイトの 2 つの攻撃は、最も一般的な侵害経路となっており、このレポートで調査されたケースの 45% を占めています。

個人情報（PII）の盗用などの**データ盗難**は、サイバー犯罪者がクラウド環境に侵入した後に最もよく実行されるアクションです。

10 億超

クラウド環境の構成ミスにより、2019 年には 10 億を超えるレコードが失われました。

ランサムウェアは、侵入されたクラウド環境で展開される最も一般的なマルウェアです。これは、2 位のクリプトマイニングと 3 位のボットネット・マルウェアの 3 倍の事例を占めています。

主な調査結果

巧妙な脅威アクターの常套手段は、多くの場合、攻撃のためのインフラストラクチャーとして**クラウド・プラットフォームを利用する**ことです。これにより、1 回のセキュリティー侵害で攻撃の効果を高めることができます。別のメリットとして、ターゲットを犠牲にして自らのコストを最小限に抑え、その他の点では正当なソースに由来しているように見せることができます。

1 時間あたり 5 万ドル超の損失

被害を受ける組織とクラウドで実行されるアプリケーションの種類に応じて、侵入は一瞬にしてこれだけ高額な利益を生み出す場合があります。

資産を再イメージ化せず、再デプロイする: 資産を再デプロイする組織は、影響を受けたクラウド環境を再イメージ化する組織と比べて、効果的なフォレンジック調査を実行できる可能性が高く、組織へのその後の被害を防ぐことができます。

多層防御が不可欠: マルウェア開発者は、クラウドの採用が増加していることを認識して、多くの一般的なクラウド・セキュリティー製品を無効にするマルウェアを作成し始めています。しかし、多くの企業は知らず知らずのうちに脆弱性を抱えたままです。

クラウド・コンピューティング: セキュリティー面での大きな利点と対処すべきリスク

オンデマンドのコンピューティング・リソースを従量課金制でインターネット経由で提供するクラウド・コンピューティングは、企業全体にコンピューティング機能を拡張することを検討している組織に多くのセキュリティー上の利点を提供します。今日、ほとんどの企業は約 20% のワークロードをクラウドに移行していますが、企業がコア IT インフラストラクチャーのモダナイズとミッション・クリティカルなデータとアプリケーションのクラウド移行を進めるにつれて、組織はこうした新しいハイブリッドなマルチクラウド環境がもたらす固有のサイバーセキュリティーの課題と機会にも対応する必要があります。

クラウド・セキュリティーについて説明する際に明確にする必要のある重要な用語があります。これらの用語は、組織がクラウドベースの資産を保護する作業を行うときに頻繁に使用されるものです。

パブリッククラウド
組織の外部でホストされるクラウド環境。

プライベートクラウド
組織内でホストおよび保守される、組織専用のクラウド環境。

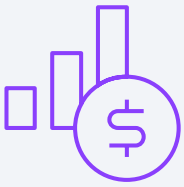
ハイブリッドクラウド
オンプレミスとオフプレミスの両方および異なるクラウド間で統合され、全体的に管理されたクラウド環境。

コンテナ化
コンテナはソフトウェアの実行単位で、アプリケーション・コードがそのライブラリーや依存関係とともに、デスクトップ、従来型 IT、クラウドのあらゆる場所で実行できるように一般的な方法でパッケージ化されています。

企業の IT 環境はますます複雑化しています。というのは、ビジネスがクラウドの要素を取り込み、そのハイブリッドなマルチクラウド・インフラストラクチャーをシンプルで、一貫性があり、統合された方法で管理する必要があるからです。しかし、アーキテクチャーで終わりではありません。データと運用がクラウドに移行されるときに、クラウドのハイパーコネクテッドな性質に内在するセキュリティー脅威を評価し、対処する必要があります。クラウドのセキュリティー脅威の状況を理解することは、組織が自らをより適切に保護し、潜在的なセキュリティー・イベントに備えるのに役立ちます。

リスクの考察

企業間でのクラウドの統合が増加する結果として、クラウド間の相互作用により、感染の可能性がオンプレミス攻撃よりもさらに速く企業全体に広がるおそれがあります。また、クラウドで実行されるデータ量に比例して、脅威アクターが盗み出す可能性があるデータ量も増えることが考えられます。データ漏えいのコストは侵害されたレコード件数と密接に関連することを考慮すると、クラウドのセキュリティー・インシデントはコストが高くなる可能性があります。コストの増加にすぐにつながる別の側面は、クラウド上の資産への不正アクセスです。侵害の種類によっては、そのアクセスにより 1 時間もかからずに 5 万ドルを超える損失が容易に発生する可能性があります。



クラウド上の資産への不正アクセスにより、

1 時間未満で 5 万ドル超の損失

が生じる可能性があります。

多くの組織にとってクラウドは新時代への取り組みです。クラウドは、組織を保護し、データ・プライバシーの懸念、規制、コンプライアンスに対処しますが、これらすべてには、従来型の IT セキュリティーの管理とは異なるベスト・プラクティスを含む、新たな適合するアプローチが求められます。

クラウド・システムを ターゲットにする攻撃者

IBM Security は、IBM X-Force Incident Response and Intelligence Services (IRIS) のインシデント対応チームを通してクラウド・システムを標的とする複数のタイプのグループを観察し、DarkOwl の仲間と協力して、ディープ・ウェブおよびダーク・ウェブ上のさらに興味深い攻撃者を発見しました。調査結果によると、金銭目的の犯罪者は最大の脅威ですが、国家的なアクターも持続的なリスクです。

金銭目的の犯罪者は、クラウド・システムをターゲットとする最大の脅威グループですが、国家的なアクターも持続的なリスクです。

クラウドをターゲットとする犯罪者

X-Force IRIS のインシデント対応データによると、クラウド環境をターゲットとする脅威アクター・カテゴリーで最も頻繁に観察されたものは、サイバー犯罪者でした。金銭目的の脅威アクターが特定のグループや組織に関係していることはめったになく、単に日和見的な攻撃でクラウド上の資産へのアクセス取得を試みるだけで、多くの場合、対象範囲をより広くするためにその試みを自動化します。ダークネットのデータ・インテリジェンス企業である DarkOwl と共同で行われたさらに詳細な調査により、地下フォーラムおよび市場にあるクラウドを標的としたサービスとアカウントの市場が盛況であることがわかりました。

アンダーグラウンドのエコシステムで扱われる主な商品として、割引価格のクラウド・サービス・アカウントがあります。たとえば、あるロシア語のフォーラムでは、大手パブリッククラウドの月額無制限のサービスを一般の販売価格よりも安く提供するベンダーが呼び物になっていました。別のケースでは、異なるアクター・グループが別の大手パブリッククラウドへのアクセス・キーをそれぞれわずか 15 ドルで販売していることが判明しました。このような種類のサービスを利用することで、脅威アクターは、その他の点では正当と思われるアカウントで、クラウド・インフラストラクチャーを悪意のある活動のために使用できるようになります。

また、犯罪者はクラウドでホストされている特定のアカウントへの侵入を支援します。英語とロシア語を話すハッカーをつなぐプラットフォームで、あるユーザーが、大手パブリッククラウド上で個人アカウントにアクセスするためのバイパス・ユーティリティーへのリンクを投稿しました。別の商品では、あるパブリッククラウドの ID を悪用する手順を詳しく説明し、そこにはハッカーがフォーラムで販売しているスクリプトが含まれていました。ダーク・ウェブとディープ・ウェブの現場で観察されるもう 1 つの市場は、クラウド・コンピューティング・リソースの販売です。たとえば、クラウド・プロバイダー・アクセスは、フィッシング・サイトをホストしようとするユーザーに販売されます。あるケースでは、ハッキング・フォーラムのメンバーが、クラウド・プロバイダーが提供する製品を模倣したパブリッククラウド環境で、フィッシング・ページをホストする計画を発表しているのがわかりました。

正規のオンライン学習コースと似せて作られたさまざまなチュートリアルもあります。ここでは、クラウド・コンピューティングのクレジットまたは盗まれたクレジット・カードを使用して、人気のあるクラウド・サービスでアカウントを開き、それらを悪用目的で使用する方法が扱われています。

国家的な攻撃

国家的な脅威アクターは、これまで金銭的利益やスパイ活動の目的でクラウド環境をターゲットとしてきました。脅威グループは、多くの場合、接続されたサードパーティー・システムにアクセスするために、クラウド環境を広範囲にわたって標的とします。

より機密性の高いデータがクラウド環境に移されるようになると、スパイ活動を中心とした脅威グループが、引き続きクラウド環境をターゲットにして戦略的インテリジェンス目標を達成することが予測されています。

脅威アクターがクラウド環境のセキュリティーを侵害する方法

他のネットワークと同様に、クラウド環境はさまざまな方法でターゲットにされる可能性があります。その方法のいくつかはクラウドに特有のものですが、多くはシステム全般に影響を与えます。

IBM Security 脅威インテリジェンス・チームは、X-Force IRIS のインシデント対応データを利用して、脅威アクターがクラウド環境をターゲットとする最も一般的な方法を発見しました。多くの場合、脅威アクターは次のメカニズムを複数使用して、アクセスを取得、維持、そして拡大させ、同じクラウド内や接続している可能性のあるクラウド上に次々とアクセス許可を拡張していきます。

クラウド・アプリケーションの脆弱性を悪用

2019 年 1 月から 2020 年 5 月にかけてクラウド環境で観察された最も一般的な侵害経路は、クラウド・アプリケーションのリモート・エクスプロイトです。これは、調査対象のクラウド関連のサイバーセキュリティー・イベントの 45% を占めています。アジャイルでスケーラブルなクラウドベースのアプリケーションは、脅威アクターにセキュリティー侵害の幅広い機会を与える可能性があります。これらのアプリケーションは、多くの場合、ビジネスの運用にも必要であるため、脅威活動の主要なターゲットになります。

45%

クラウド環境の**リモート・エクスプロイト**は、観察された最も一般的な感染経路であり、調査対象のクラウド関連のサイバーセキュリティー・イベントの 45% を占めています。

過去 2 年間、IBM Security は、環境内に脆弱なアプリケーションが存在しているが検出されないという複数のインシデントに対応してきました。それはクラウド内のセキュリティーの成熟不足が原因であることもありますが、多くの場合、「シャドー IT」が原因である可能性があります。これは、従業員が承認外でクラウドを利用し、脆弱なクラウド・アプリケーションを使用することを選択したため、環境全体が危険にさらされる状態を指します。

クラウド環境でリモートの脆弱性に対処することは、発見された問題の一覧が公開されていないことも一因となって、困難となっていました。2020 年まで、クラウド製品の脆弱性は従来の CVE の範囲外でした。つまり、クラウド・インフラストラクチャーに関連する脆弱性が公開されたり、長期にわたって記録されたりすることはほとんどありませんでした。その結果、クラウド環境は以前に認識されていたものよりもずっと脆弱であり、対処されていないさまざまな問題が潜んでいる可能性があります。

構成ミスの悪用

IBM の 2020 年版 X-Force 脅威インテリジェンス・インデックスのデータによると、2019 年に、脅威アクターは誤って構成されたクラウド・サーバーを利用して、侵害された環境から 10 億を超えるレコードを不正流出させました。クラウド環境の構成ミスとそれに続くデータ漏えいは、依然として全般的に記録損失の最大原因の 1 つです。そうしたミスは組織のクラウド内の資産に影響を与える可能性があり、脅威アクターはそれらの組織から機密情報に素早くアクセスして盗み出すことができます。

10 億超の盗み出されたレコード

脅威アクターは、2019 年に、誤って設定されたクラウド・サーバーを利用して、侵害されたクラウド環境から 10 億を超えるレコードを不正流出させました。

IBM X-Force 脅威インテリジェンス・インデックス

クラウド間のセキュリティー侵害

脅威アクターは、1 つのクラウド環境を感染させてクラウド環境を侵害した後、信頼できる接続を使用して他のクラウドに横方向に展開し、さらに別のクラウド環境を感染させることがあります。

このクラウド間のセキュリティー侵害は特に狡猾です。なぜなら、クラウド環境、特に大手パブリッククラウドは、多くの場合、通信量が多く、この種の感染を検出することがより困難になる可能性があるからです。

ある X-Force IRIS インシデント対応では、さまざまな地域に指定されたクラウド間で転送されるデータ量が通常よりも多いことが観察されたときに、脅威アクターが検出されました。このタイプの攻撃では、脅威アクターは大規模なデータ・リポジトリー間を素早く移動し、多くの検出メカニズムを回避して、全体的な運用上の活動に自らの攻撃アクションを隠しながら、ターゲットの企業全体に危害を加えることができました。

遡上

別のタイプの侵害経路では、脅威アクターが、基盤となるハードウェアに侵入することでクラウド・リポジトリーへの特権アクセスを取得しようとしていることがわかりました。

この「遡上」という手法では、脅威アクターはクラウド環境への最初のアクセスを取得し、次に基盤となるホストにアクセスし、さらに管理システムに到達してクライアント環境間を移動する必要があります。管理者は多くの場合、インスタンス間でデータを移動する必要もあるため、遡上は脅威アクターの活動を正当な管理活動として隠すことがあります。そのため、この 2 つを区別することは複雑になる場合があります。この手法は、2020 年に 10 点満点を獲得するような重大な脆弱性が公開されたときに明らかになりました。この欠陥により、脅威アクターはクラウド環境内のハードウェアベースの分離を破壊して、コードの傍受、プログラムの操作、そして同じハードウェアでホストされている他のユーザーのアクティビティーに影響を与えることができました。この欠陥は修正されました。

脅威アクターがクラウドを使用してセキュリティーを侵害する方法

クラウド環境で一度だけ危害をもたらす理論的手法は多くありますが、IBM Security では、脅威アクターが従来のさまざまな攻撃戦術を使用して、この新しいテクノロジーの強化された機能から利益を得ようとしていることがわかっています。

ランサムウェア、データの盗難、およびクリプトマイニングは、クラウドを利用しながら、組織に害を及ぼす主要な方法です。ただし、クラウド環境でマルウェアや詐欺サイトをホスティングしたり、ワームを利用して他のクラウドを感染させたりすることで、脅威アクターは組織自体の範囲外に広範な被害を引き起すことに加え、接続している当事者に対するリスクも悪化させることが可能です。

ランサムウェア

2019 年から 2020 年にわたって分析された X-Force IRIS インシデント対応のケースでは、ランサムウェアはクラウドに展開されたマルウェアの中で間違いなく最も一般的なタイプであり、それ以外のマルウェアの 3 倍のインシデントに相当します。

ランサムウェアの使用は 3 倍でした。

IBM のインシデント対応のケース調査に基づいて、クラウドに展開されたその他のマルウェアと比較した結果です。

従来のネットワーク化されたエンドポイントに対するランサムウェア攻撃とは異なり、クラウド内のランサムウェアの影響はより破壊的で、より大きなデータ損失を引き起こす可能性があります。その原因は、クラウド環境でサポートされている幅広い運用、重要なアプリケーションへの潜在的な影響、そして毎日クラウドを経由する膨大なデータ量によるものと考えられます。

X-Force IRIS が対応したランサムウェアのインシデントでは、インフラストラクチャー・プロバイダーとそのクライアントの間のクラウド管理責任のギャップが原因で感染が発生しました。このギャップは、セキュリティー侵害が長期間検出されない事態を引き起こし、組織へのコストが増加しました。また、プロバイダーとクライアントの両方にクラウド・セキュリティーの役割を定義することの重要性が浮き彫りになりました。

データの盗難

クラウド環境は大量の情報をホストしています。このデータが脅威アクターによって盗まれ、地下市場で販売される可能性があります。IBM X-Force IRIS が扱ったインシデントから、盗まれたデータの種類はさまざまであることがわかりました。たとえば、クラウド・データの漏えいから、脅威アクターがクレジット・カード番号などの機密性の高い PII を盗んでいることが判明しました。別のインシデントでは、侵害されたクラウドからクライアント関連の電子メールが盗まれる可能性があることもわかっています。

データの盗難は、2019 年に IBM X-Force が侵害されたクラウド環境で観察した最も一般的な脅威アクティビティーの第 2 位に挙がっています。

盗まれるデータのタイプは、脅威アクターの動機と巧妙さに基づいてさまざまですが、クラウド環境では、使用可能なデータの量がはるかに多いため、侵害によって受ける損害もそれだけ大きくなる可能性があります。

クリプトマイニング

不正なクリプトマイニングの脅威、特にクラウドなどの拡張されたインフラストラクチャーを利用するものに関して、IBM X-Force IRIS は過去 1 年にわたって、脅威アクターがクラウド環境を使用して暗号通貨をマイニングする複数のインスタンスを観察してきました。

2019 年に、X-Force IRIS が対応したインシデントのケースでは、クラウド・サーバーがクリプトマイナーによって感染し、その後、接続されたマシンに横方向に拡散しようとしました。この種のセキュリティー侵害は、いくつかの影響を与える可能性があります。オンプレミス・クラウド環境の場合、電力コストの増加やハードウェア・コンポーネントの劣化を早めるほかに、パフォーマンスへの影響があります。パフォーマンスに関しては、むしろ金融セクターなどの業界で重要になる可能性があります。

外部／パブリッククラウドでは、データ使用量の増加や、処理能力の低下によって応答時間の遅延が生じるため、請求料金の増加が発生する可能性があります。いずれの場合も、クリプトマイニングは組織リソースの損失であり、ビジネス運用を妨げる可能性があります。

マルウェアまたは悪意のあるサイトのホスト

脅威アクターは、侵害されたクラウド環境を使用してマルウェアをホストし、その後、他の環境に拡散する可能性があります。たとえば、2019 年後半に、犯罪者はクラウド・プラットフォームでクレジット・カード・スキマーをホストし、それは後で標的のマシンにダウンロードされました。別のケースでは、脅威アクターが 1 つのクラウド・インスタンスで 200 を超える技術サポート詐欺サイトをホストし、ユーザーをこれらのサイトに誘導し、クラウド環境を使用して攻撃を正当なものと見せかけました。

マルウェアや悪意のあるサイトをクラウド環境でホストすると、正当なインフラストラクチャーへの接続要求として表示され、脅威アクターはネットワーク・ブロックを回避することができます。また、クラウド・ホスティングを使用することで、脅威アクターは抽象化レイヤーを得て、攻撃キャンペーンの活動追跡がより困難になります。組織が知らないうちにクラウドでマルウェアをホストしている場合、特にそれが長期間に及ぶ場合、組織はデータそのものを失うだけでなく、この活動が持続するのを許容したとして非難される可能性もあるため、直接的な被害と評判への悪影響の両方につながるおそれがあります。

DNS のセキュリティー侵害

IBM X-Force IRIS は、脅威アクターがクラウドにホストしている DNS サービスを侵害して、従業員を別のサイトにリダイレクトする複数のインシデントを観察しました。

DNS キャッシュ・ポイズニングの概念を利用するこの狡猾な攻撃方法は、既存のクラウド・アクセスを利用して組織にさらに危害を加え、ユーザーが検出するのが困難になる可能性があります。このタイプのセキュリティー侵害では、ブラウザーを悪用して悪意のあるペイロードをエンドポイント・マシンにドロップしようとするサイトにユーザーをリダイレクトしたり、フィッシング・サイトにリダイレクトしてネットワーク資格情報を盗んだりする可能性があります。場合によっては、広告へのリダイレクトまたはクリック詐欺が、犯罪者の私腹を肥やすように設定されています。

DNS セキュリティー侵害は新しい攻撃ではありませんが、組織がこれらのサービスを外部のクラウド・プロバイダーにシフトし続けると、脅威アクターはセキュリティー侵害につながる可能性のある新しい経路を発見でき、その影響は組織全体に広がる可能性があります。

水平展開

脅威アクターはさまざまな方法を使用して、初期感染からクラウド環境の他の部分、またはクラウド・リソースにアクセスするエンドポイント・ボックスにまで拡大してきました。2019 年に、IBM X-Force IRIS が対応したインシデントでは、クラウド環境に展開されたマルウェアが SSH ブルートフォース攻撃で他のマシンに拡散しようとして、クラウドにアクセスする外部のローカル・マシンに影響を与えました。

また、2019 年に、Exim サーバーを介して拡散する Linux ワームである Exim ワームが、CVE 2019-10149 のリモート・エクスプロイトにより自動的に感染を拡散したことが報告されています。ワームは、クリプトジャッキング・マルウェアをサーバーにドロップすることを目的にサーバーを乗っ取ります。

この種の水平展開は、クラウド感染の影響を悪化させ、組織の内部ネットワーク空間にその影響をもたらす可能性があります。

クラウドネイティブのマルウェアとその進化

多くのクラウドベースのシステムは、オンプレミスのオペレーティング・システムとアプリケーションと同じオペレーティング・システムとアプリケーションを実行しているため、クラウド環境で作用することが検出されているマルウェアの多くは、クラウドの外部で検出されたものと同じです。ただし、クラウド・システムをターゲットとするか、またはクラウド・システムを利用するように特別に設計されたマルウェアのインスタンスがあります。

これらのマルウェアの亜種は次の 3 つのグループに分類されます。

— クラウドを使用して拡張するマルウェア

— クラウド環境に適応するマルウェア

— 運用インフラストラクチャーにクラウド環境を使用するマルウェア

クラウドを使用して拡張するマルウェア

マルウェアのオペレーターは、クラウド・アプリケーションまたはプラットフォームを特にターゲットとすることで、1 回のセキュリティー侵害で素早く攻撃の効果を高め、大きな利益を得ることができます。新しいクラウドの現実に適応するマルウェア・ファミリーの 1 つの例は、2018 年 10 月に報告された Linux ベースのボットである DemonBot です。DemonBot は、Hadoop を実行しているクラウド・サーバーをターゲットとし、Hadoop のリソース管理ツールの脆弱性を利用して感染させます。

X-Force IRIS は、クラウド環境で検出された DemonBot のインスタンスを調査しました。このケースでは、料金とリソース使用量の大幅な増加が原因で、組織が被害を受けていることが判明しました。このケースでは、DemonBot バイナリーの主な機能は、ボットネットの一部として分散型サービス妨害 (Distributed Denial of Service: DDoS) 攻撃を仕掛けることでした。マルウェアのオペレーターは、クラウドをターゲットとする機能を追加することで、クラウド・リソースを使用してこれらの攻撃を増強できます。

組織のクラウド導入で使用されている別のマルウェア・ファミリーは、2019 年 10 月に特定されたクリプトマイニング・ワームである Graboid です。このマルウェアは、セキュリティーで保護されていない Docker ホストをターゲットとして侵害し、そこに悪意のある Docker コンテナをダウンロードしました。この悪意のあるコンテナはクリプトマイニングを実行し、さらにマルウェアを他のホストに拡散しました。

2019 年 6 月に、研究者は、誤って構成された Docker ホストをターゲットとして、そこに侵入する攻撃キャンペーンについて報告しました。この場合、API の構成ミスを悪用して脆弱なコンテナにマルウェアを展開したのは、AESDDoS と呼ばれる Linux ボットネット・マルウェアでした。このマルウェアは、コマンド・コントロール・サーバーからコマンドを受信し、さまざまな DDoS 攻撃を仕掛けることができました。

クラウド環境に適応するマルウェア

過去 2 年間に、Intezer の研究者は、主にクラウド環境で、Linux サーバーをターゲットとするサイバー攻撃の数の大幅な増加を観察しました。Linux オペレーティング・システムは、全クラウド・サーバーのほぼ 90% を占めています。

マルウェアを使用してクラウドをターゲットとする脅威アクターの 1 つの例は、中国系の Pacha Group です。このグループは、これまで検出されていなかった Linux の新しいマルウェア亜種を使用して、クラウドベースのインフラストラクチャーを標的にしています。GreedyAntd は、大量のコードを以前の亜種と共有します。クラウド環境で Linux ベースのファイル・ストレージ・システム (NAS サーバー) をターゲットとする別のマルウェアは、QNAPCrypt ランサムウェアです。この種の脅威は、非常に大規模なユーザー・ベースに影響を与え、クラウドでホストされている大量のデータに損害を与える可能性があります。

クラウド環境の人気が高まり続けるにつれて、Linux を対象としたマルウェアが増加し続ける可能性があります。

運用インフラストラクチャーにクラウド環境を使用するマルウェア

組織が運用を拡大させるのと同じように、特に組織犯罪や国家的攻撃に関連するマルウェアを配布する攻撃者も運用を拡大することを選択できます。X-Force IRIS は、マルウェアの操作のためにクラウド環境をさまざまな方法で利用する脅威アクターを観察しました。

1 つの調査は RokRat に関するものです。これは韓国の被害者を標的とすることが観察され、ITG10 (別名 APT37、Scarcruft) に起因するリモート・アクセス・ツール (RAT) です。この攻撃では、ペイロードと C2 通信のホスティングに正当な商用クラウド・ストレージ・サービスが使用されていました。組織のネットワークは通常の運用の一部として重要なクラウド通信を行い、正当なプロバイダーをホワイトリストに登録するため、インフラストラクチャーにこのクラウド・サービスを使用することは検出するのが難しい可能性があります。そのようなクラウド環境でマルウェアをホストすることにより、悪意のあるペイロードのダウンロードを検出することも困難になります。

RokRat と同様に、Karae は ITG10 に起因する別のバックドアです。これも C2 通信にクラウド・ストレージ・プロバイダーを使用することで知られています。X-Force IRIS によって分析された Karae のサンプルでは、正当なクラウド・ストレージ・サービス・プロバイダーが脅威アクターによってマルウェアをホストするために使用され、アカウントの認証情報がマルウェアのバイナリーにハードコーディングされていました。Karae は被害者のシステムに関する情報を収集し、それをファイルに書き込んでから、クラウドにアップロードします。また、このサービスから追加のバイナリーをダウンロードして実行しようとします。

この戦術では、通常の正当なユーザー・アクティビティーと混ざり合う可能性があるため、一般的に検出の問題が生じます。そのことは、さまざまな動機を持つマルウェア・オペレーターがこの戦術を使用することを選ぶ理由でもあります。

クラウドのセキュリティーを強化するための推奨事項

クラウド環境でのセキュリティー・インシデントへの対応には、通常の方法でのインシデント対応以外に特別な考慮が求められます。この分野での X-Force IRIS の豊富な経験に基づいて、クラウド・インシデントへの準備と対応時に学んだ重要な教訓をまとめました。

より安全なクラウド環境の準備

結末を念頭に置いて開始する

ワークロードやデータをクラウドに移動することを検討する前に、その目的に関する計画を作成します。構想プロセスにセキュリティー制御を組み込み、クラウドで実行される操作の重要性と機密性を考慮に入れましょう。プログラムを開発するときには、ハイブリッドクラウドのセキュリティーに関するすべての側面の可視性と制御を得るのに役立つ、包括的なセキュリティー・サービスを提供するパートナーの活用を検討しましょう。

プロアクティブなシミュレーションを使用する

クラウド環境内で予期されるセキュリティー・イベントと予期されないセキュリティー・イベントの両方をシミュレートして、準備の有効性を把握しましょう。この準備では、社内の対応手順集と標準の操作手順を演習する機会を得ることができます。技術と運用の両面での対応スキルのテストと改善に重点を置くことにより、組織は、被害が発生または拡大する前に問題の解決に迅速に取り組むことができます。さらに、これらの演習を侵害指標（Indicator of Compromise: IOC）などの戦術情報で補強することで、脅威インテリジェンスによる対応シナリオを補強することができます。

ポリシーの「デッド・スポット」を防止する

外部クラウドの場合、クラウド環境を保護する責任は、多くの場合、組織とクラウド・ホスティング・プロバイダーの両方にあります。クラウド・ホスティングが設定するだけで終わりのサービスであることはめったにありません。クラウド・サービス・プロバイダーとサービスを使用する組織の両方の側にセキュリティーが必要です。契約の交渉時に各当事者の役割を明確にしておくことは、インシデントの前に責任、制御、監視、および潜在的な法的責任を定義するのに役立ちます。これにより、ポリシーのギャップに起因するインシデントを防ぐだけでなく、より効率的な検出とインシデント対応を可能にすることができます。

クラウド・セキュリティーにベスト・プラクティスを適用する

クラウド・セキュリティーには独自のアプローチがありますが、いくつかの点で他のネットワークのセキュリティーにも似ています。したがって、クラウドがセキュリティー侵害の影響を受けずに済むことはないため、組織はセキュリティーのベスト・プラクティスをクラウド環境に適用する必要があります。不正アクセスの脅威を軽減するために、多要素認証を実装すると、盗まれた資格情報を使用した侵入を防ぐことができます。

特権アカウント管理（PAM）は、クラウドの保護を強化するためのもう 1 つの重要な考え方です。アカウントを必要最小限の特権に制限して、アカウントの侵害による被害を最小限に抑えてください。また、ゼロトラスト・モデルの採用を検討してください。これらのプラクティスをクラウド環境に実装することで、組織はインシデントのリスクを軽減したり、潜在的なセキュリティー・イベントの影響を削減したりできます。

監視とログ

クラウド環境は、さまざまな問題に対応するために監視が必要です。適切な監視は、クラウド・スプロール、サードパーティーのアクセス、予期しない故障など、マルウェアや攻撃の初期の兆候の検出に役立ちます。クラウド・ユーザーは、悪意のある活動のフォレンジック調査に備えて、クラウド環境のイベントの安定したロギングを維持する必要があります。サービスを開始する前に、組織とクラウド・ホスティング・プロバイダーの間でクラウド・イベントの監視とロギングの責任を定義して、ポリシーのデッド・スポットを防ぐようにしましょう。

脅威インテリジェンスを使用して脅威を監視する

脅威アクターは進化を続け、戦術、技術、手順という既存の武器を、特にクラウド環境をターゲットとした新しい機能により増強させています。こうした機能の開発が続いているため、組織は脅威インテリジェンスを活用して、ターゲットの変化を監視し、効果的な防御を実装する必要があります。

クラウド・セキュリティー・インシデントへの効果的な対応

再イメージ化ではなく再デプロイする

組織はクラウド・インスタンスを終了すると、潜在的価値のあるフォレンジック・アーティファクトを失います。このデータを即座に破壊するのではなく、影響を受けるシステムを分離して既知のクリーンなイメージを立ち上げることにより、フォレンジック調査員は感染したインスタンスを分析し、問題とそれを将来防止する方法を理解するための手掛かりをさらに発見することができます。

インシデントが発生した場合、調査員が作業を実行できるようにクラウド内にワークステーションを構築し、侵害されたサーバーからイメージを作成して、揮発性メモリー・データを収集します。また、根本原因のフォレンジック分析を行うと、IT 管理者は汚染されたベース・イメージを再展開できなくなる可能性があります。

高額な転送コストを念頭に置く

組織が今日直面している課題の 1 つは、インシデントの後に大規模なサーバー・イメージをダウンロードすると、クラウド環境から外向きのデータ移動に伴う高額な転送のため、法外なコストがかかる可能性があるということです。インシデントの前に関連するポリシーまたは要件を設定しておくと、特に感染が同じクラウド上の他のインスタンスに害を及ぼす可能性がある場合に、ダウンロードのコストを削減できます。

適切な調査ツールを用意する

クラウド・セキュリティーには、問題が発生した場合に徹底的な調査を実行するための適切なツールが必要です。多くの一般的なインシデント対応ツールやフォレンジック・ツールは、ローカル環境またはオンプレミスでホストされているサーバーでのみ有効であり、クラウド環境には対応していません。しかし、適切なツールキットを準備すると、効果的なクラウド調査が可能になります。

さらに、組織はインシデント対応計画全体にクラウド資産を含め、クラウド・セキュリティー・インシデント対応を戦術レベルでテストして、用意したツールが使用中のすべてのクラウド環境で機能することを確認する必要があります。

インシデント対応を自動化する

イベントへの手動対応に頼るのではなく、クラウド環境に効果的なセキュリティーの自動化を実装すると、検出能力と対応能力を向上させることができます。たとえば、Infrastructure as Code (IaC) のアプローチに従い、CloudFormation、宣言的アプローチ、サーバーレスのイベント駆動型 Lambda サービスなどのツールを使用することで、侵害された組織は事前定義されたテンプレートから環境を効率的に再構築することができます。この方法では、その環境に対するランサムウェア攻撃や破壊的サイバー攻撃の間に迅速な回復を実現できる可能性があります。

結論

ベンダーからインフラストラクチャーを契約するユーザーにとって、クラウド・セキュリティーは、クラウド・サービスのプロバイダーとユーザーの両方による共同の取り組みです。クラウドで運用する組織は、クラウド環境に対する脅威を認識して、データとサービスを適切に保護する必要があります。

IBM X-Force の調査によると、組織がクラウド・インフラストラクチャーに移行していることを脅威アクターも鋭く意識しており、それに応じて進化しています。クラウド侵害の被害コストは増大し続けているため、組織はクラウドベースの資産を保護するための対策を講じる必要があります。組織はプロアクティブに行動し、推奨される措置を講じることで、適切な防御とともにクラウドベースの世界へと移行することができます。

IBM X-Force について

IBM X-Force は、最新の脅威動向を調査および監視し、新たな脅威や重大な脅威についてお客様や一般市民に助言し、IBM のお客様を保護するために役立つセキュリティー・コンテンツを配信します。インフラストラクチャー、データ、アプリケーションの保護から、クラウドおよびマネージド・セキュリティー・サービスまで、IBM Security Services には、重要な資産を保護するための専門知識があります。IBM Security は、有能な人材を採用し、世界で最も高度なネットワークのいくつかを保護しています。

IBM X-Force IRIS について

脚注

1. Methodology Caveat: このレポートで引用した統計では、2018 年 6 月から 2020 年 3 月までの X-Force IRIS のインシデント対応レポートのサブセットが使用されています。 この制限は、プライバシーの問題を含むさまざまな理由により必要となりました。そのため、ここに含まれる統計は、この期間中にクラウド・セキュリティーで観察された、より広範な傾向を反映しているものの、収集の偏りの影響をある程度受けている可能性があります。

IBM Security

調査協力

Intezer
DarkOwl

IBM Security
New Orchard Rd
Armonk, NY 10504

Produced in the United States of America
June 2020

IBM