ORACLE CLOUD

Oracle CASB Cloud Service の機械学習を使用した脅威検出

US CERT (United States - Computer Emergency Readiness Team)[i]が最近発表したアナウンスメント(2018 年 4 月 16 日発行)によると、ロシアをベースとした IP アドレスから、米国ベースのインフラ(個人のネットワークに接続されたホーム・ルーターなどのデバイスを含む)への侵入が盛んに試みられていると報告されており、同局が警告を呼びかけています。このような国家支援型の攻撃は、リソースが国家レベルで利用できるという性質上、検出や防護が最も困難な攻撃の一種と言えます。多くの人々は、自分がこの種の攻撃の対象になる可能性は低いと思っていますが、これらの脅威によってさまざまな副作用が生じることは少なくありません。楽観的な考え方は、包括的な情報セキュリティ(InfoSec) ・リスクマネジメントには効果的で持続可能なアプローチとは言えません。しかし残念ながら、クラウド・アプリケーションを使用する企業の多くでは、インターネットベースの脅威に対し、依然としてこのような楽観的アプローチがとられています。

多くの攻撃タイプに共通する戦術の 1 つとして、"ロー・ボリューム" (限られたトランザクション数)と"ロー・ベロシティ" (限られたターゲット数)でトランザクションを実行する手法がありますが、この種の攻撃は、稼働率の高いクラウド・サービスでは検出が困難な場合があります。この種の攻撃が国家によって大規模に実行された場合、それらを検出し、防護することはいっそう困難になる可能性があります。そこで大きな役割を果たすことになるのが、機械学習と人工知能です。実際、Oracle Cloud Access Security Broker (CASB)を導入している企業では、この種の攻撃を検出したり、担当チームにそのことを通知するなどして、その機能が活用されています。

攻撃の発生源と行動パターン

F5 Networks の報告によると、2018 年 6 月 11 日から 12 日[ii]にかけて、シンガポールベースのリソースに対するサイバー攻撃が増加したとされています。これは、米国の大統領が北朝鮮のリーダーとの会談のために同国を訪問した期間です。この調査結果を受け、F5 Networks では、米国大統領が今後外国を訪問する際にも、その滞在期間中に攻撃が増加するかどうかについて、注目を強めるようになりました。

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com. Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

ORACLE

2018 年 7 月 19 日に F5 Networks が発行した記事[iii]は、米国とロシアの両大統領の会談期間中にフィンランドのリソースに対して実行された情報セキュリティ攻撃に関するものでした。F5 Networks によって報告された攻撃の大部分は IoT デバイスを狙った"ブルートフォース攻撃"でしたが、その他の未知のエンティティからは、フィンランドベースの組織で使用されているクラウド環境の資格証明を抽出し、リソースを侵害しようとする攻撃も実行されていました。

稼働率の高いクラウド・サービスに対して国家がロー・ボリューム、ロー・ベロシティの攻撃を実行した場合、攻撃者が使用できるリソースの規模を考えると、それらの攻撃を検出することは非常に困難になる可能性があります。Oracle CASB では、認証トークンを使ったこの種の攻撃を検出した実績があります。以下にその詳細を示します。

ORACLE CASB で検出された認証トークンの脅威

オラクルの CASB は、フィンランドベースの複数の組織で導入されているクラウド・サービスを監視するために使用されていますが、このところ、異常なアクティビティが増加していることが確認されています。実際、フィンランドに本拠を置く、ある CASB カスタマには、ユーザー認証トークンのリプレイを試みる攻撃者によって主要クラウド・サービスのユーザー・アカウントに脅威が生じている旨のアラートが送られました。怪しい IP アドレスから実行されたこれらのロー・ボリュームなトークン・リプレイ試行を受け、さらなる調査を実施しました。その結果、IP レピュテーションが関連付けられていない場所から、類似の試行が行われていることがわかりました。

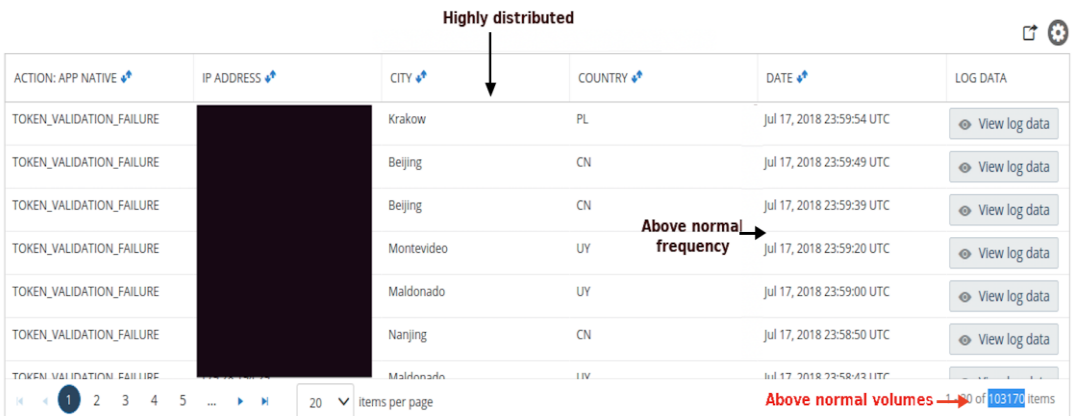

図 1: Oracle CASB によって検出された異常アクティビティ

仮想トークンは、認証と信頼関係の確立のためにエンティティ間で使用されます。トークンが侵害された場合、悪意のあるトランザクションが有効なトランザクションとして処理される可能性があります。トークン検証エラーは、通常の操作の一部として発生する場合もあります。たとえば、トークンが期限切れになった場合、それ以降にそのトークンを使おうとすると、検証でエラーが返されます。多くの攻撃タイプに共通する戦術の 1 つとして、"ロー・ボリューム"と"ロー・ベロシティ"でトランザクションを実行する手法がありますが、この種の攻撃は、使用率の高いシステムでは検出が困難な場合があります。今回の一連のイベントでは、脅威検出システムによってアクターを特定できる可能

Authored by Oracle CASB Threat Labs

性があることがわかりました。トークン検証エラーは複数検出されましたが、24 時間に各トークンについて検出されたリプレイ・イベントは、1〜3 件に過ぎませんでした。

オラクルの CASB では、ヘルシンキ・サミットの 90 日前から開催期間にかけて、650 GB 以上のクラウド・セキュリティ・データが消費・分析されました。サミットの少し前から開催期間にかけては、お客様の監視対象クラウド・サービスに対する攻撃の件数に、かなりの増加が見られました。Oracle CASB では、トークン検証エラーの件数の増加が検出され、アラートが送信されました。具体的には、下記の図 2 に示すように、1 つの国からのエラーが 700%も増加しました。

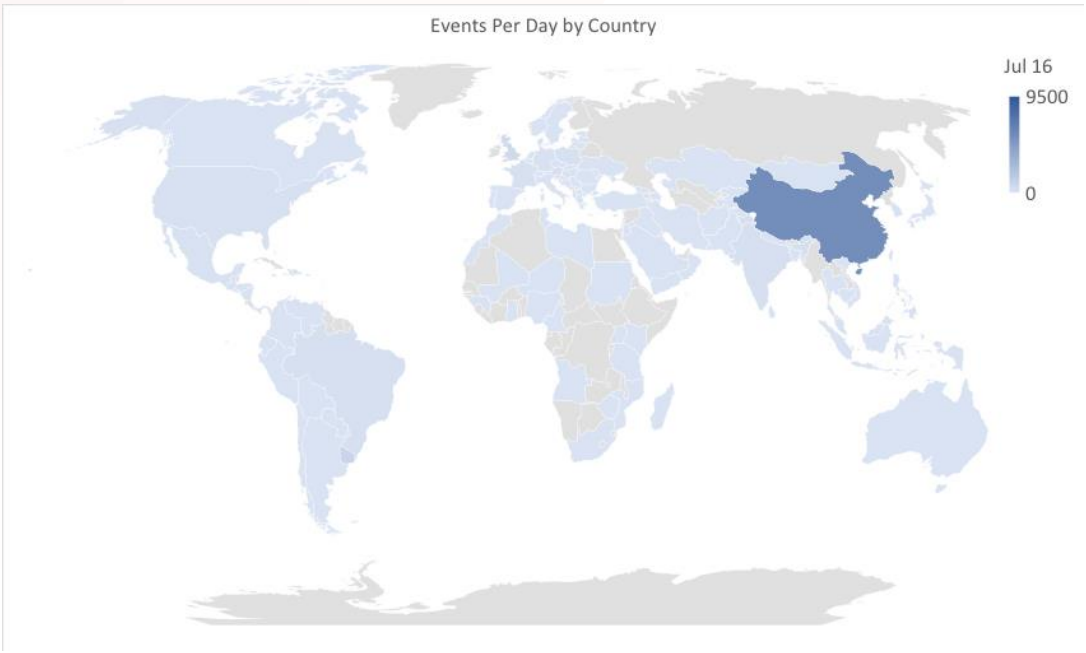

図 2: ヘルシンキ・サミット開催日(7 月 16 日)に発生した国別のイベント数

中国を発生源とする異常アクティビティをさらに調べたところ、多くの IP アドレスにおいて、1 日の間に異常な数のイベントが一貫して発生しており、前日や翌日にもアクティビティの増加が見られないことがわかりました。下記の図 3 をご覧ください。イベントのアプローチ方法が高度に標準化されている場合や、規模に一貫性がある場合、また特定のイベント・タイプに偏っている場合は、発生源がプログラムである可能性が高いと言えます。人間が操作した場合、このようなパターンのアクティビティが生成されることはほとんどありません。また、トークン・リプレイ攻撃で数百個の IP アドレスを循環させるアプリケーションが大規模に使用されている場合は、アクターの技術が高度であるものと考えられます。

Authored by Oracle CASB Threat Labs

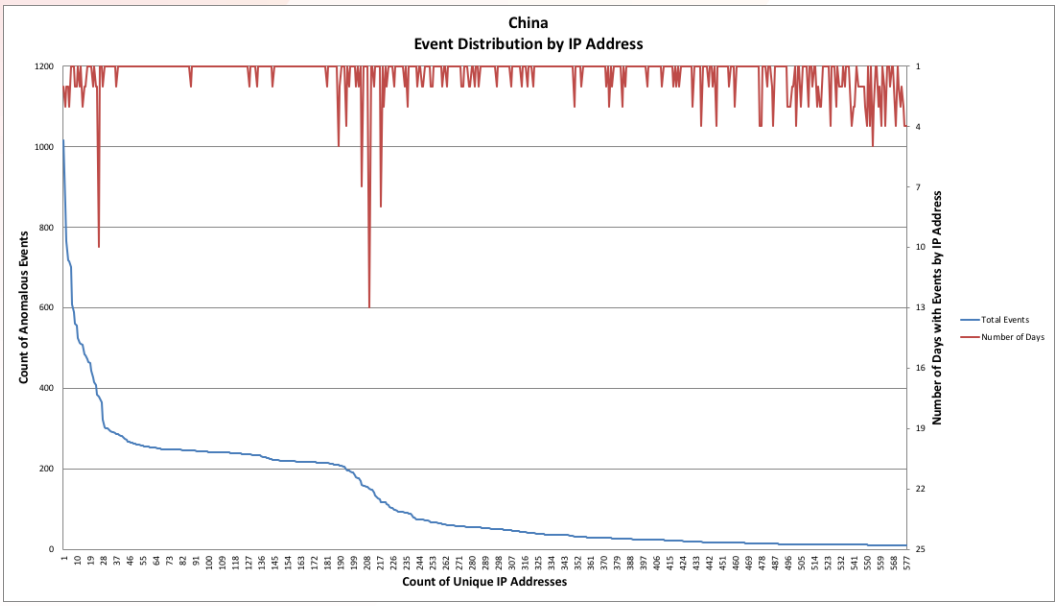

図 3: IP アドレス別のイベント分布(中国)

一方、フィンランドからのアクティビティについては、下記の図 4 を見てわかるように、イベントの数が日によってばらついており、同じ時間枠や同様のユニーク IP アドレス数で見ても、分布状況が大きく異なっています。

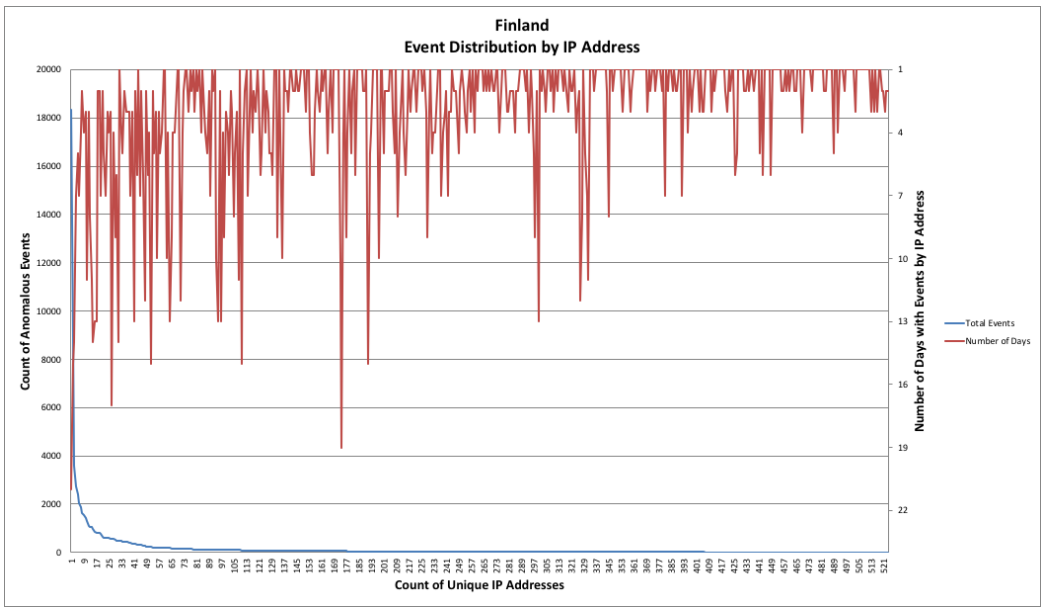

図 4: IP アドレス別のイベント分布(フィンランド)

Authored by Oracle CASB Threat Labs

限られた数の IP アドレスから大量のアクティビティが発生している場合、それらのトランザクションはその組織の IP 範囲内から発生しているものと考えられます。1 つの国(この場合は中国)からのアクティビティに均一性が見られる場合、その特長は図 3: IP アドレスと比べても簡単に区別できます。

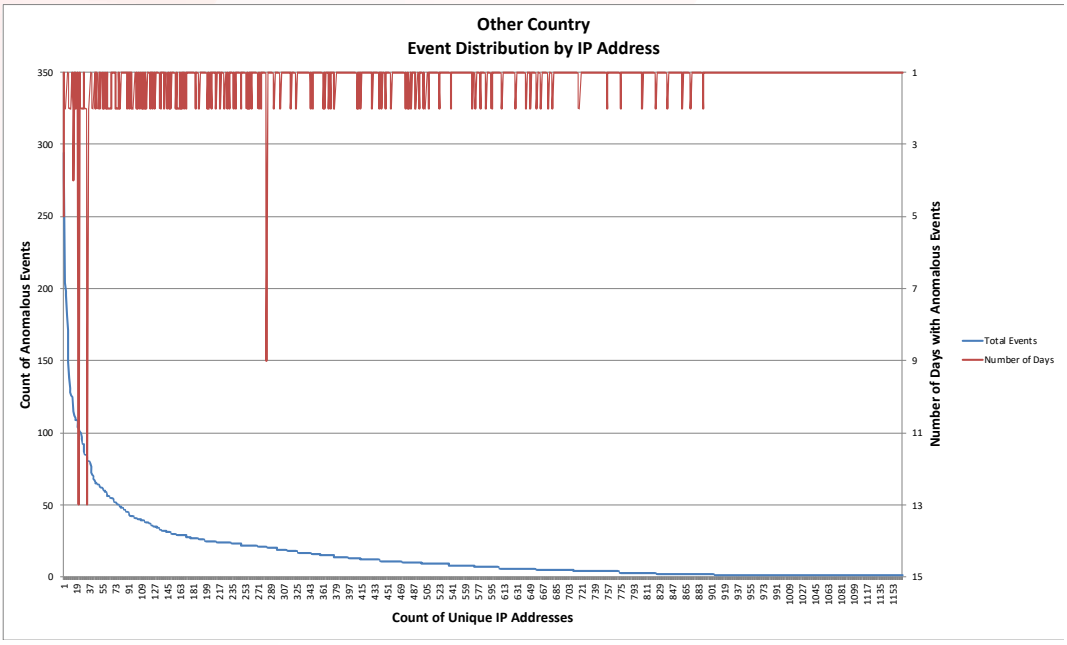

図 5: イベントの均一性

さらに調査を行ったところ、上記の図 5 が示すように、"ロー・ボリューム"、"ロー・ベロシティ"のプロービングが増えていることがわかりました。この例の場合、人為的な一貫性が見られるアクティビティが、複数の IP アドレスによってミラーリングされています。このことから、標準的な脅威検出システムのしきい値を超えないような方法で、クラウド・アプリケーションを活発にプローブしていることがうかがえます。

まとめ

異常なアクティビティを監視し、それらを調査するには、包括的な情報セキュリティ・プログラムを開発し、チームをトレーニングすることが重要です。機械学習を使った自動化ツール(オラクルの CASB Cloud Service など)は、大量のデータやトランザクションが処理されるクラウド・アプリケーションの性質を踏まえ、高度な分析を実行できるように設計されています。これにより、外部アクターからの怪しい活動と有効な承認済みユーザーの活動を区別し、異常を特定して、チームにアラートを送信できるようになっています。機械学習を活用すれば、内部の脅威や異常なユーザー行動を検出するための高速なメカニズムを提供できます。

[i] https://www.us-cert.gov/ncas/alerts/TA18-106A
[ii] https://www.f5.com/labs/articles/threat-intelligence/russian-attacks-against-singapore-spike-during-trump-kim-summit
[iii] https://www.f5.com/labs/articles/threat-intelligence/cyber-attacks-spike-in-finland-before-trump-putin-meeting

Authored by Oracle CASB Threat Labs