翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。

GuardDuty EC2 の検出結果タイプ

PDF (guardduty-ug.pdf#guardduty_finding-types-ec2) | **RSS (amazon-guardduty-doc-history.rss)**

次の検出結果は Amazon EC2 リソースに固有であり、常に `Instance` のリソースタイプを有しています。検出結果の重要度と詳細は、EC2 インスタンスが不審なアクティビティの対象であるか、不審なアクティビティを実行するアクターであるかを示すリソースロールによって異なります。

ここにリストされている検出結果には、検出結果タイプの生成に使用されるデータソースとモデルが含まれます。データソースとモデルの詳細については、「基礎データソース (./guardduty_data-sources.html) 」を参照してください。

注記

インスタンスが既に終了している場合、または基盤となる API コールが、異なるリージョンに EC2 インスタンスを生じるクロスリージョン API コールの一部である場合、インスタンスの詳細がEC2 インスタンスの検出結果から欠落することがあります。

すべての EC2 の検出結果について、問題のリソースを調べて正常に動作しているかどうかを確認することをお勧めします。アクティビティが認可されると、そのリソースに対する誤検出の通知を防ぐため、抑制ルールや信頼できる IP リストを使用できます。予期しないアクティビティについては、セキュリティのベストプラクティスとしてインスタンスが侵害されていると仮定し、侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) で説明されている対策をとることをお勧めします。

トピック

- Backdoor:EC2/C&CActivity.B (#backdoor-ec2-ccactivityb)
- Backdoor:EC2/C&CActivity.B!DNS (#backdoor-ec2-ccactivitybdns)
- Backdoor:EC2/DenialOfService.Dns (#backdoor-ec2-denialofservicedns)
- Backdoor:EC2/DenialOfService.Tcp (#backdoor-ec2-denialofservicetcp)
- Backdoor:EC2/DenialOfService.Udp (#backdoor-ec2-denialofserviceudp)
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts (#backdoor-ec2-denialofserviceudpontcpports)
- Backdoor:EC2/DenialOfService.UnusualProtocol (#backdoor-ec2-denialofserviceunusualprotocol)
- Backdoor:EC2/Spambot (#backdoor-ec2-spambot)
- Behavior:EC2/NetworkPortUnusual (#behavior-ec2-networkportunusual)
- Behavior:EC2/TrafficVolumeUnusual (#behavior-ec2-trafficvolumeunusual)
- CryptoCurrency:EC2/BitcoinTool.B (#cryptocurrency-ec2-bitcointoolb)
- CryptoCurrency:EC2/BitcoinTool.B!DNS (#cryptocurrency-ec2-bitcointoolbdns)
- DefenseEvasion:EC2/UnusualDNSResolver (#defenseevasion-ec2-unusualdnsresolver)
- DefenseEvasion:EC2/UnusualDoHActivity (#defenseevasion-ec2-unusualdohactivity)
- DefenseEvasion:EC2/UnusualDoTActivity (#defenseevasion-ec2-unusualdotactivity)
- Impact:EC2/AbusedDomainRequest.Reputation (#impact-ec2-abuseddomainrequestreputation)
- Impact:EC2/BitcoinDomainRequest.Reputation (#impact-ec2-bitcoindomainrequestreputation)
- Impact:EC2/MaliciousDomainRequest.Reputation (#impact-ec2-maliciousdomainrequestreputation)
- Impact:EC2/PortSweep (#impact-ec2-portsweep)
- Impact:EC2/SuspiciousDomainRequest.Reputation (#impact-ec2-suspiciousdomainrequestreputation)
- Impact:EC2/WinRMBruteForce (#impact-ec2-winrmbruteforce)
- Recon:EC2/PortProbeEMRUnprotectedPort (#recon-ec2-portprobeemrunprotectedport)

- Recon:EC2/PortProbeUnprotectedPort (#recon-ec2-portprobeunprotectedport)
- Recon:EC2/Portscan (#recon-ec2-portscan)
- Trojan:EC2/BlackholeTraffic (#trojan-ec2-blackholetraffic)
- Trojan:EC2/BlackholeTraffic!DNS (#trojan-ec2-blackholetrafficdns)
- Trojan:EC2/DGADomainRequest.B (#trojan-ec2-dgadomainrequestb)
- Trojan:EC2/DGADomainRequest.C!DNS (#trojan-ec2-dgadomainrequestcdns)
- Trojan:EC2/DNSDataExfiltration (#trojan-ec2-dnsdataexfiltration)
- Trojan:EC2/DriveBySourceTraffic!DNS (#trojan-ec2-drivebysourcetrafficdns)
- Trojan:EC2/DropPoint (#trojan-ec2-droppoint)
- Trojan:EC2/DropPoint!DNS (#trojan-ec2-droppointdns)
- Trojan:EC2/PhishingDomainRequest!DNS (#trojan-ec2-phishingdomainrequestdns)
- UnauthorizedAccess:EC2/MaliciousIPCaller.Custom (#unauthorizedaccess-ec2-maliciousipcallercustom)
- UnauthorizedAccess:EC2/MetadataDNSRebind (#unauthorizedaccess-ec2-metadatadnsrebind)
- UnauthorizedAccess:EC2/RDPBruteForce (#unauthorizedaccess-ec2-rdpbruteforce)
- UnauthorizedAccess:EC2/SSHBruteForce (#unauthorizedaccess-ec2-sshbruteforce)
- UnauthorizedAccess:EC2/TorClient (#unauthorizedaccess-ec2-torclient)
- UnauthorizedAccess:EC2/TorRelay (#unauthorizedaccess-ec2-torrelay)

Backdoor:EC2/C&CActivity.B

EC2 インスタンスは、既知の C&C サーバーに関連付けられる IP をクエリしています。

デフォルトの重要度: [High] (高)

- **データソース:** VPC フローログ

この検出結果は、AWS 環境のリスト化したインスタンスが既知の C&C サーバーに関連付けられた IP をクエリしていることを知らせるものです。リスト化

したインスタンスは侵害されている可能性があります。C&C サーバーは、ボットネットのメンバーにコマンドを発行するコンピュータです。

ボットネットとは、一般的なタイプのマルウェアに感染し制御されたインターネットコネクテッドデバイス (PC、サーバー、モバイルデバイス、IoT デバイスなど) のコレクションです。通常、ボットネットは、マルウェアの配布や盗用された情報 (クレジットカード番号など) の収集に使用されます。ボットネットの目的と構造によっては、C&C サーバーから分散型サービス拒否 (DDoS) 攻撃を開始するためのコマンドが発行されることもあります。

> **注記**
>
> クエリされた IP が log4j 関連の場合、関連付けられた検出結果のフィールドには次の値が含まれます。
>
> - service.additionalInfothreatListName .= Amazon
> - service.additionalInfo.threatName = Log4j Related

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Backdoor:EC2/C&CActivity.B!DNS

EC2 インスタンスが、既知の C&C サーバーに関連付けられるドメイン名をクエリしています。

デフォルトの重要度: [High] (高)

- **データソース;** DNS ログ

この検出結果は、AWS 環境のリスト化したインスタンスが既知の C&C サーバーに関連付けられているドメインをクエリしていることを知らせるものです。リスト化したインスタンスは侵害されている可能性があります。C&C サーバーは、ボットネットのメンバーにコマンドを発行するコンピュータです。

ボットネットとは、一般的なタイプのマルウェアに感染し制御されたインターネットコネクテッドデバイス (PC、サーバー、モバイルデバイス、IoT デバイス

など) のコレクションです。通常、ボットネットは、マルウェアの配布や盗用された情報 (クレジットカード番号など) の収集に使用されます。ボットネットの目的と構造によっては、C&C サーバーから分散型サービス拒否 (DDoS) 攻撃を開始するためのコマンドが発行されることもあります。

> **注記**
>
> クエリされたドメイン名が log4j 関連の場合、関連付けられた検出結果のフィールドには次の値が含まれます。
>
> - service.additionalInfothreatListName .= Amazon
> - service.additionalInfo.threatName = Log4j Related

> **注記**
>
> がこの検出結果タイプ GuardDuty を生成する方法をテストするには、テストドメイン に対してインスタンスから DNS リクエストを行います (`dig` Linux の場合は 、Windows `nslookup` の場合は を使用） `guarddutyc2activityb.com`。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Backdoor:EC2/DenialOfService.Dns

EC2 インスタンスが、DNS プロトコルを使用したサービス拒否 (DoS) 攻撃の実行に利用されている可能性があります。

デフォルトの重要度: [High] (高)

- **データソース:** VPC フローログ

この検出結果は、大量のアウトバウンド DNS トラフィックを生成しているリスト化した EC2 インスタンスが AWS 環境にあることを知らせるものです。これは、リストされたインスタンスが侵害され、DNS プロトコルを使用した

denial-of-service (DoS) 攻撃の実行に利用されていることを示している可能性があります。 DoS

> **注記**
>
> この検出結果では、パブリックにルーティング可能な IP アドレスに対する DoS 攻撃のみ検出しています。このような IP アドレスは、DoS 攻撃の主なターゲットとなっています。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Backdoor:EC2/DenialOfService.Tcp

EC2 インスタンスが TCP プロトコルを使用したサービス拒否 (DoS) 攻撃の実行に利用されている可能性があります。

デフォルトの重要度: [High] (高)

- **データソース:** VPC フローログ

この検出結果は、大量のアウトバウンド TCP トラフィックを生成しているリスト化した EC2 インスタンスが AWS 環境にあることを知らせるものです。これは、インスタンスが侵害され、TCP プロトコルを使用した denial-of-service (DoS) 攻撃の実行に利用されていることを示している可能性があります。

> **注記**
>
> この検出結果では、パブリックにルーティング可能な IP アドレスに対する DoS 攻撃のみ検出しています。このような IP アドレスは、DoS 攻撃の主なターゲットとなっています。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon

EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Backdoor:EC2/DenialOfService.Udp

EC2 インスタンスが UDP プロトコルを使用したサービス拒否 (DoS) 攻撃の実行に利用されている可能性があります。

デフォルトの重要度: [High] (高)

- **データソース:** VPC フローログ

この検出結果は、大量のアウトバウンド UDP トラフィックを生成しているリスト化した EC2 インスタンスが AWS 環境にあることを知らせるものです。これは、リストされたインスタンスが侵害され、UDP プロトコルを使用した denial-of-service (DoS) 攻撃の実行に利用されていることを示している可能性があります。

> **注記**
>
> この検出結果では、パブリックにルーティング可能な IP アドレスに対する DoS 攻撃のみ検出しています。このような IP アドレスは、DoS 攻撃の主なターゲットとなっています。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Backdoor:EC2/DenialOfService.UdpOnTcpPorts

EC2 インスタンスが、TCP ポートで UDP プロトコルを使用したサービス拒否 (DoS) 攻撃の実行に利用されている可能性があります。

デフォルトの重要度: [High] (高)

- **データソース:** VPC フローログ

この検出結果は、TCP 通信に通常使用されるポートを対象とした大量のアウトバウンド UDP トラフィックを生成している EC2 インスタンスが AWS 環境にあることを知らせるものです。これは、リストされたインスタンスが侵害され、TCP ポートで UDP プロトコルを使用して (DoS) 攻撃を実行する denial-of-serviceために使用されていることを示している可能性があります。

> **注記**
>
> この検出結果では、パブリックにルーティング可能な IP アドレスに対する DoS 攻撃のみ検出しています。このような IP アドレスは、DoS 攻撃の主なターゲットとなっています。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Backdoor:EC2/DenialOfService.UnusualProtocol

EC2 インスタンスが、異常なプロトコルを使用したサービス拒否 (DoS) 攻撃の実行に利用されている可能性があります。

デフォルトの重要度: [High] (高)

- **データソース:** VPC フローログ

この検出結果は、ご利用の AWS 環境にリストされている EC2 インスタンスが、Internet Group Management Protocol などの EC2 インスタンスでは通常使用されない異常なプロトコルタイプから大量のアウトバウンドトラフィックを生成していることを知らせるものです。これは、インスタンスが侵害され、異常なプロトコルを使用した denial-of-service (DoS) 攻撃の実行に利用されていることを示している可能性があります。この検出結果では、パブリックにルーティング可能な IP アドレスに対する DoS 攻撃のみ検出しています。このような IP アドレスは、DoS 攻撃の主なターゲットとなっています。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Backdoor:EC2/Spambot

EC2 インスタンスがポート 25 でリモートホストと通信して異常な動作を示しています。

デフォルトの重要度: [Medium] (中)

- **データソース:** VPC フローログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスがポート 25 でリモートホストと通信していることを知らせるものです。この EC2 インスタンスにはポート 25 での通信履歴が以前にないため、この動作は通常と異なります。従来、ポート 25 はメールサーバーで SMTP 通信のために使用されています。この検出結果は、EC2 インスタンスが侵害されており、スパムの送信に利用されている可能性があることを示しています。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Behavior:EC2/NetworkPortUnusual

EC2 インスタンスが通常と異なるサーバーポートでリモートホストと通信しています。

デフォルトの重要度: [Medium] (中)

- **データソース:** VPC フローログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスが、確立されたベースラインから逸脱して動いていることを知らせるものです。この EC2 イン

スタンスには、このリモートポートでの通信履歴がありません。

> **注記**
>
> EC2 インスタンスがポート 389 またはポート 1389 で通信した場合、関連する検出の重要度は [High] (高) に変更され、検出結果フィールドには次の値が含まれます。
>
> - service.additionalInfo.context = Possible log4j callback

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Behavior:EC2/TrafficVolumeUnusual

EC2 インスタンスがリモートホストに対して通常と異なる大量のネットワークトラフィックを生成しています。

デフォルトの重要度: [Medium] (中)

- **データソース:** VPC フローログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスが、確立されたベースラインから逸脱して動いていることを知らせるものです。この EC2 インスタンスでは、このリモートホストに対してこれほど大量のトラフィックを送信した履歴がありません。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

CryptoCurrency:EC2/BitcoinTool.B

EC2 インスタンスが暗号通貨関連のアクティビティに関連付けられている IP アドレスをクエリしています。

デフォルトの重要度: [High] (高)

- **データソース:** VPC フローログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスでビットコインやその他の暗号通貨関連アクティビティに紐づけられた IP アドレスがクエリされていることを知らせるものです。ビットコインは、他の通貨、製品、サービスと交換できる国際的な暗号通貨およびデジタル決済システムです。ビットコインはビットコインマイニングの報酬であり、脅威アクターを高度に追及します。

修復のレコメンデーション

暗号通貨の情報を取り出して管理するためこの EC2 インスタンスがを使用する場合、またはこのインスタンスがブロックチェーンのアクティビティに関与している場合は、この検出結果はご利用の環境の想定されるアクティビティを示している可能性があります。ご利用の AWS 環境でこのような状況が発生した場合は、この検出結果に対する抑制ルールを設定することをお勧めします。抑制ルールは、2 つのフィルター条件で構成する必要があります。1 つ目の条件では、**[Finding type]** (結果タイプ) 属性に `CryptoCurrency:EC2/BitcoinTool.B` という値を使用します。2 つ目のフィルター条件では、ブロックチェーンのアクティビティに関係するインスタンスの **[Instance ID]** (インスタンス ID) を使用します。抑制ルールの作成の詳細については、「抑制ルール (./findings_suppression-rule.html) 」を参照してください。

このアクティビティが予期しないものである場合は、インスタンスが侵害されている可能性があります。「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

CryptoCurrency:EC2/BitcoinTool.B!DNS

EC2 インスタンスが暗号通貨関連のアクティビティに関連付けられているドメイン名をクエリしています。

デフォルトの重要度: [High] (高)

- **データソース;** DNS ログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスで、ビットコイン、またはその他の暗号通貨関連アクティビティに紐づけたドメインがクエリされていることを知らせるものです。ビットコインは、他の通貨、製品、サービスと交換できる国際的な暗号通貨およびデジタル決済システムです。ビットコインはビットコインマイニングの報酬であり、脅威アクターを高度に追及します。

修復のレコメンデーション

暗号通貨の情報を取り出して管理するためこの EC2 インスタンスがを使用する場合、またはこのインスタンスがブロックチェーンのアクティビティに関与している場合は、この検出結果はご利用の環境の想定されるアクティビティを示している可能性があります。ご利用の AWS 環境でこのような状況が発生した場合は、この検出結果に対する抑制ルールを設定することをお勧めします。抑制ルールは、2 つのフィルター条件で構成する必要があります。1 つ目の条件では、**[Finding type]** (結果タイプ) 属性に `CryptoCurrency:EC2/BitcoinTool.B!DNS` という値を使用します。2 つ目のフィルター条件では、ブロックチェーンのアクティビティに関係するインスタンスの **[Instance ID]** (インスタンス ID) を使用します。抑制ルールの作成の詳細については、「抑制ルール (./findings_suppression-rule.html) 」を参照してください。

このアクティビティが予期しないものである場合は、インスタンスが侵害されている可能性があります。「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

DefenseEvasion:EC2/UnusualDNSResolver

Amazon EC2 インスタンスでは、例外的なパブリック DNS リゾルバーと通信しています。

デフォルトの重要度: [Medium] (中)

- **データソース:** VPC フローログ

この検出結果は、AWS 環境のリスト化した Amazon EC2 インスタンスが、ベースラインの動作から逸脱して動いていることを知らせるものです。この EC2 インスタンスには、このパブリック DNS リゾルバーに対する最近の通信履歴がありません。 GuardDuty コンソールの検出結果の詳細パネルの **Unusual** フィールドには、クエリされた DNS リゾルバーに関する情報が表示されます。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

DefenseEvasion:EC2/UnusualDoHActivity

Amazon EC2 インスタンスが、例外的な DNS over HTTPS (DoH) 通信を実行しています。

デフォルトの重要度: [Medium] (中)

- **データソース:** VPC フローログ

この検出結果は、AWS 環境内のリスト化した Amazon EC2 インスタンスが、確立されたベースラインから逸脱して動いていることを知らせるものです。この EC2 インスタンスには、このパブリック DoH サーバーとの DNS over HTTPS (DoH) 通信の最近の履歴はありません。検出結果の詳細の **[例外的]** フィールドには、問い合わせた DoH サーバーに関する情報が表示されます。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

DefenseEvasion:EC2/UnusualDoTActivity

Amazon EC2 インスタンスが、例外的な DNS over TLS (DoT) 通信を実行しています。

デフォルトの重要度: [Medium] (中)

- **データソース:** VPC フローログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスが、確立されたベースラインから逸脱して動いていることを知らせるものです。この EC2 インスタンスには、このパブリック DoT サーバーとの DNS over TLS (DoT) 通信の

最近の履歴はありません。検出結果詳細パネルの **[例外的]** フィールドには、問い合わせた DoT サーバーに関する情報が表示されます。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Impact:EC2/AbusedDomainRequest.Reputation

EC2 インスタンスが、既知の悪用されたドメインに関連付けられた評価の低いドメイン名をクエリしています。

デフォルトの重要度: [Medium] (中)

- **データソース;** DNS ログ

この検出結果は、AWS 環境内にリストされている Amazon EC2 インスタンスが、既知の悪用されたドメインまたは IP アドレスに関連付けられたレピュテーションの低いドメイン名をクエリしていることを知らせるものです。悪用したドメインの例としては、動的 DNS プロバイダーだけでなく、無料のサブドメイン登録を提供する最上位のドメイン名 (TLD) と第 2 位のドメイン名 (2LD) があります。脅威アクターは、無料または低コストでドメインを登録するこれらのサービスを使用する傾向があります。このカテゴリの評価の低いドメインは、レジストラのパーキング IP アドレスを決定する有効期限切れドメインであり、アクティブになっていない可能性があります。パーキング IP は、レジストラがどのサービスにもリンクされていないドメインのトラフィックを管理する場所です。脅威アクターが一般的にこれらのレジストラのサービスまたは C&C のサービス、マルウェア配布に使用するため、リストされた Amazon EC2 インスタンスは侵害される可能性があります。

[Low] (低) のレピュテーションドメインは、レピュテーションスコアモデルに基づいています。このモデルは、ドメインの特徴を評価およびランク付けし、それが悪意のあるものである可能性を判断します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon

EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Impact:EC2/BitcoinDomainRequest.Reputation

EC2 インスタンスが、暗号通貨関連のアクティビティに関連付けられている評判の低いドメイン名をクエリしています。

デフォルトの重要度: [High] (高)

- **データソース;** DNS ログ

この検出結果は、AWS 環境のリスト化した Amazon EC2 インスタンスで、ビットコイン、またはその他の暗号通貨関連アクティビティに紐づけた評判の低いドメイン名がクエリされていることを知らせるものです。ビットコインは、他の通貨、製品、サービスと交換できる国際的な暗号通貨およびデジタル決済システムです。ビットコインはビットコインマイニングの報酬であり、脅威アクターを高度に追及します。

[Low] (低) のレピュテーションドメインは、レピュテーションスコアモデルに基づいています。このモデルは、ドメインの特徴を評価およびランク付けし、それが悪意のあるものである可能性を判断します。

修復のレコメンデーション

暗号通貨の情報を取り出して管理するためこの EC2 インスタンスがを使用する場合、またはこのインスタンスがブロックチェーンのアクティビティに関与している場合は、この検出結果はご利用の環境の想定されるアクティビティを示している可能性があります。ご利用の AWS 環境でこのような状況が発生した場合は、この検出結果に対する抑制ルールを設定することをお勧めします。抑制ルールは、2 つのフィルター条件で構成する必要があります。1 つ目の条件では、**[Finding type]** (結果タイプ) 属性に `Impact:EC2/BitcoinDomainRequest.Reputation` という値を使用します。2 つ目のフィルター条件では、ブロックチェーンのアクティビティに関係するインスタンスの **[Instance ID]** (インスタンス ID) を使用します。抑制ルールの作成の詳細については、「抑制ルール (./findings_suppression-rule.html) 」を参照してください。

このアクティビティが予期しないものである場合は、インスタンスが侵害されている可能性があります。「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Impact:EC2/MaliciousDomainRequest.Reputation

EC2 インスタンスが、悪意のある既知のドメインに関連付けられた評判の低いドメインをクエリしています。

デフォルトの重要度: [High] (高)

- **データソース;** DNS ログ

この検出結果は、AWS 環境内にリストされている Amazon EC2 インスタンスが、悪意のある既知のドメインまたは IP アドレスに関連付けられたレピュテーションの低いドメイン名をクエリしていることを知らせるものです。例えば、ドメインを既知のシンクホール IP アドレスに関連付けることができます。シンクホールドメインは、以前に脅威アクターに制御されたドメインであり、ドメインへのリクエストは、インスタンスが侵害されていることを示している場合があります。これらのドメインは、悪意のある既知のキャンペーンやドメイン生成アルゴリズムと相関している可能性もあります。

[Low] (低) のレピュテーションドメインは、レピュテーションスコアモデルに基づいています。このモデルは、ドメインの特徴を評価およびランク付けし、それが悪意のあるものである可能性を判断します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Impact:EC2/PortSweep

EC2 インスタンスが、多数の IP アドレスのポートを調査しています。

デフォルトの重要度: [High] (高)

- **データソース:** VPC フローログ

この検出結果は、AWS 環境にリスト化した EC2 インスタンスが、多数のパブリックにルーティング可能な IP アドレス上のポートを調査していることを知らせるものです。このアクティビティタイプは、通常脆弱性ホストを見つけて悪用するのに使われます。 GuardDuty コンソールの検出結果の詳細パネルには、最新のリモート IP アドレスのみが表示されます。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Impact:EC2/SuspiciousDomainRequest.Reputation

EC2 インスタンスが、年齢や低人気により、本質的に疑わしい、低評判のドメイン名をクエリしています。

デフォルトの重要度: [Low] (低)

- **データソース;** DNS ログ

この検出結果は、AWS 環境のリスト化した Amazon EC2 インスタンスが悪意があると疑われたり、過去に悪意のあるドメインだったため評判の低いドメイン名をクエリしていることを知らせるものですが、当社の評判モデルは、既知の脅威と明確に関連付けることができませんでした。これらのドメインは通常、新たに観察されるか、または少量のトラフィックを受信します。

[Low] (低) のレピュテーションドメインは、レピュテーションスコアモデルに基づいています。このモデルは、ドメインの特徴を評価およびランク付けし、それが悪意のあるものである可能性を判断します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Impact:EC2/WinRMBruteForce

EC2 インスタンスがアウトバウンドの Windows リモート管理総当たり攻撃を実行しています。

デフォルトの重要度: [Low] (低)*

> **注記**
>
> EC2 インスタンスが総当たり攻撃の対象である場合、この検出結果の重要度は「低」です。EC2 インスタンスが総当たり攻撃の動作主体である場合、この検出結果の重要度は「高」です。

- **データソース:** VPC フローログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスが、Windows ベースのシステム上の Windows リモート管理サービスへのアクセスを目的とした Windows リモート管理 (WinRM) 総当たり攻撃を実行していることを知らせるものです。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Recon:EC2/PortProbeEMRUnprotectedPort

EC2 インスタンスの保護されていない EMR 関連のポートを悪意のある既知のホストが探しています。

デフォルトの重要度: [High] (高)

- **データソース:** VPC フローログ

この検出結果は、 AWS環境のクラスターの一部であるリスト化した EC2 インスタンスの EMR 関連の機密ポートが、セキュリティグループ、アクセスコントロールリスト (ACL)、または Linux IPTables などのオンホストファイアウォールによってブロックされていないことを知らせるものです。この検出結果は、

インターネット上の既知のスキャナーがこのポートを積極的に調査していることも知らせるものです。ポート 8088 (YARN ウェブ UI ポート) など、この検出結果をトリガーできるポートは、リモートコード実行で使用される可能性があります。

修復のレコメンデーション

インターネットからクラスター上のポートへのオープンアクセスをブロックし、それらのポートへのアクセスを必要とする特定の IP アドレスのみにアクセスを制限する必要があります。詳細については、「Security Groups for EMR Clusters (https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-security-groups.html) 」(EMR クラスターのセキュリティグループ) を参照してください。

Recon:EC2/PortProbeUnprotectedPort

EC2 インスタンスの保護されていないポートを悪意のある既知のホストが探しています。

デフォルトの重要度: [Low] (低)*

> **注記**
>
> この検出結果のデフォルトの重要度は [Low] (低) です。ただし、調査対象のポートが Elasticsearch (9200 または 9300) で使用されている場合、検出結果の重要度は High になります。

- **データソース:** VPC フローログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスのポートが、セキュリティグループ、アクセスコントロールリスト (ACL)、Linux IPTables など、ホスト上のファイアウォールでブロックされておらず、インターネットの既知のスキャナーが積極的に調査していることを知らせるものです。

識別された保護されていないポートが 22 または 3389 であり、それらのポートを使用してインスタンスに接続している場合は、それらのポートへのアクセスを自社ネットワークの IP アドレス空間の IP アドレスのみに許可することで公開を制限することができます。Linux でポート 22 へのアクセスを制限するには、「Linux インスタンス用の受信トラフィックの認可 (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-

instance.html) 」を参照してください。Windows でポート 3389 へのアクセスを制限するには、「Windows インスタンス用の受信トラフィックの認可 (https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/authorizing-access-to-an-instance.html) 」を参照してください。

GuardDuty は、ポート 443 および 80 に対してこの検出結果を生成しません。

修復のレコメンデーション

インスタンスがウェブサーバーをホストしている場合など、インスタンスが意図的に公開されている場合があります。ご利用の AWS 環境でこのような状況が発生した場合は、この検出結果に対する抑制ルールを設定することをお勧めします。抑制ルールは、2 つのフィルター条件で構成する必要があります。1 つ目の条件では、**[Finding type]** (結果タイプ) 属性に `Recon:EC2/PortProbeUnprotectedPort` という値を使用します。2 番目のフィルター条件は、要塞ホストとして機能する 1 つ以上のインスタンスと一致する必要があります。これらのツールをホストするインスタンスで識別可能な条件に応じて、**[Instance image ID]** (インスタンスイメージ ID) 属性または **[Tag]** (タグ) 値の属性のいずれかを使用できます。抑制ルールの作成の詳細については、「抑制ルール (./findings_suppression-rule.html) 」を参照してください。

このアクティビティが予期しないものである場合は、インスタンスが侵害されている可能性があります。「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Recon:EC2/Portscan

EC2 インスタンスがリモートホストにアウトバウンドポートスキャンを実行しています。

デフォルトの重要度: [Medium] (中)

- **データソース:** VPC フローログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスが短時間にに複数のポートに接続しようとして、ポートスキャン攻撃を行っている可能性があることを知らせるものです。ポートスキャン攻撃の目的は、オープンポートを見つけ、マシンで実行されているサービスを発見してそのオペレーティングシステムを特定することです。

修復のレコメンデーション

この検出結果は、ご利用の環境の EC2 インスタンスに脆弱性評価アプリケーションがデプロイされており、それらのアプリケーションがポートをスキャンして、誤ってオープンポート設定になっているものをアラートするので、誤検出される可能性があります。ご利用の AWS 環境でこのような状況が発生した場合は、この検出結果に対する抑制ルールを設定することをお勧めします。抑制ルールは、2 つのフィルター条件で構成する必要があります。1 つ目の条件では、**[Finding type]** (結果タイプ) 属性に `Recon:EC2/Portscan` という値を使用します。2 番目のフィルター条件は、これらの脆弱性評価ツールをホストする 1 つ以上のインスタンスと一致する必要があります。これらのツールをホストするインスタンスで識別可能な条件に応じて、**[Instance image ID]** (インスタンスイメージ ID) 属性または **[Tag]** (タグ) 値の属性のいずれかを使用できます。抑制ルールの作成の詳細については、「抑制ルール (./findings_suppression-rule.html) 」を参照してください。

このアクティビティが予期しないものである場合は、インスタンスが侵害されている可能性があります。「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Trojan:EC2/BlackholeTraffic

EC2 インスタンスが既知のブラックホールであるリモートホストの IP アドレスに通信しようとしています。

デフォルトの重要度: [Medium] (中)

- **データソース:** VPC フローログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスがブラックホール (あるいはシンクホール) の IP アドレスと通信しようとしているため、侵害されている可能性があることを知らせるものです。ブラックホールとは、送受信トラフィックが密かに破棄されるネットワークの場所を指し、意図した受信者にデータが届いていないことは送信元に知らされません。ブラックホール IP アドレスは、稼働していないホストマシンやホストが割り当てられていないアドレスを指定します。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon

EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Trojan:EC2/BlackholeTraffic!DNS

EC2 インスタンスがブラックホールの IP アドレスにリダイレクトされるドメイン名をクエリしています。

デフォルトの重要度: [Medium] (中)

- **データソース;** DNS ログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスがブラックホール IP アドレスにリダイレクトされるドメイン名をクエリしているため、侵害されている可能性があることを知らせるものです。ブラックホールとは、送受信トラフィックが密かに破棄されるネットワークの場所を指し、意図した受信者にデータが届いていないことは送信元に知らされません。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Trojan:EC2/DGADomainRequest.B

EC2 インスタンスがアルゴリズムを使用して生成されたドメインをクエリしています。このようなドメインは、マルウェアによって悪用されることが多く、EC2 インスタンスが侵害されている場合があります。

デフォルトの重要度: [High] (高)

- **データソース;** DNS ログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスがドメイン生成アルゴリズム (DGA) のドメインをクエリしようとしていることを知らせるものです。EC2 インスタンスは侵害されている可能性があります。

DGA は、大量のドメイン名を定期的に生成してコマンドアンドコントロール (C&C) サーバーとのランデブーポイントとするために使用されます。C&C サーバーは、ボットネットのメンバーにコマンドを発行するコンピュータであり、一般的なタイプのマルウェアに感染して制御されたインターネットのコネクテッドデバイスのコレクションです。ランデブーポイントの候補数が多いと、感染されたコンピュータは毎日これらのドメイン名の一部にアクセスしてアップデートやコマンドを受け取ろうとするため、ボットネットを効果的にシャットダウンすることが困難となります。

> **注記**
>
> この検出結果は、アドバンストな経験則を使用したドメイン名分析に基づいており、脅威インテリジェンスフィードでは検出されない新しい DGA ドメインを識別する可能性があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Trojan:EC2/DGADomainRequest.C!DNS

EC2 インスタンスがアルゴリズムを使用して生成されたドメインをクエリしています。このようなドメインは、マルウェアによって悪用されることが多く、EC2 インスタンスが侵害されている場合があります。

デフォルトの重要度: [High] (高)

- **データソース;** DNS ログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスがドメイン生成アルゴリズム (DGA) のドメインをクエリしようとしていることを知らせるものです。EC2 インスタンスは侵害されている可能性があります。

DGA は、大量のドメイン名を定期的に生成してコマンドアンドコントロール (C&C) サーバーとのランデブーポイントとするために使用されます。C&C サーバーは、ボットネットのメンバーにコマンドを発行するコンピュータであり、一般的なタイプのマルウェアに感染して制御されたインターネットのコネクテ

ッドデバイスのコレクションです。ランデブーポイントの候補数が多いと、感染されたコンピュータは毎日これらのドメイン名の一部にアクセスしてアップデートやコマンドを受け取ろうとするため、ボットネットを効果的にシャットダウンすることが困難となります。

> **注記**
>
> この検出結果は、 の脅威インテリジェンスフィードの既知の DGA GuardDutyドメインに基づいています。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Trojan:EC2/DNSDataExfiltration

EC2 インスタンスが DNS クエリを使用してデータを密かに抽出しようとしています。

デフォルトの重要度: [High] (高)

- **データソース;** DNS ログ

この検出結果は、AWS 環境のリスト化した EC2 インスタンスが、アウトバウンドデータ転送用の DNS クエリを使用しているマルウェアであることを知らせるものです。このタイプのデータ転送は、侵害されたインスタンスを示し、データの漏洩につながる可能性があります 通常、DNS トラフィックはファイアウォールでブロックされません。例えば、侵害された EC2 インスタンスのマルウェアは、データ (クレジットカード番号など) を DNS クエリ内にエンコードし、それを攻撃者が制御するリモート DNS サーバーに送信できます。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Trojan:EC2/DriveBySourceTraffic!DNS

EC2 インスタンスがドライブバイダウンロード攻撃の既知の攻撃元であるリモートホストのドメイン名をクエリしています。

デフォルトの重要度: [High] (高)

- **データソース;** DNS ログ

この検出結果は、自動ダウンロード攻撃の既知のソースであるリモートホストのドメイン名をクエリしているため、リスト化した AWS 環境の EC2 インスタンスが侵害された可能性があることを知らせるものです。これらは、インターネットから意図せずにダウンロードされるコンピュータソフトウェアであり、ウイルス、スパイウェア、マルウェアの自動インストールをトリガーする場合があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Trojan:EC2/DropPoint

EC2 インスタンスが、マルウェアによって収集された認証情報やその他の盗難されたデータを保持していることが認識されているリモートホストの IP アドレスに通信しようとしています。

デフォルトの重要度: [Medium] (中)

- **データソース:** VPC フローログ

この検出結果は、AWS 環境の EC2 インスタンスで、マルウェアが取り込んだ認証情報やその他の盗難されたデータを保持して、リモートホストの IP アドレスに通信しようとしていることを知らせるものです。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Trojan:EC2/DropPoint!DNS

EC2 インスタンスが、マルウェアによって収集された認証情報やその他の盗難されたデータを保持していることが認識されているリモートホストのドメイン名をクエリしています。

デフォルトの重要度: [Medium] (中)

- **データソース;** DNS ログ

この検出結果は、AWS 環境の EC2 インスタンスで、マルウェアが取り込んだ認証情報やその他の盗難されたデータを保持するリモートホストのドメイン名をクエリしていることを知らせるものです。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

Trojan:EC2/PhishingDomainRequest!DNS

EC2 インスタンスがフィッシング攻撃に関与しているドメインをクエリしています。EC2 インスタンスは侵害されている可能性があります。

デフォルトの重要度: [High] (高)

- **データソース;** DNS ログ

この検出結果は、AWS 環境の EC2 インスタンスがフィッシング攻撃に関与しているドメインをクエリしようとしていることを知らせるものです。フィッシングドメインは、個人を特定できる情報、銀行やクレジットカードの詳細情報とパスワードなど、ユーザーが機密データを提供するように仕向ける、正当な

機関になりすました人物によって設定されます。EC2 インスタンスがフィッシングウェブサイトに保存されている機密データを検索しようとしたり、フィッシングウェブサイトを設定しようとしたりする可能性があります。EC2 インスタンスは侵害されている可能性があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

EC2 インスタンスがカスタム脅威リストの IP アドレスに接続しています。

デフォルトの重要度: [Medium] (中)

- **データソース:** VPC フローログ

この検出結果は、AWS 環境の EC2 インスタンスが、ユーザーがアップロードした脅威リストに含まれている IP アドレスを使用してアウトバウンド通信していることを知らせるものです。 GuardDuty で、脅威リストは既知の悪意のある IP アドレスで構成されます。 GuardDuty は、アップロードされた脅威リストに基づいて結果を生成します。この検出結果を生成するために使用された脅威リストは、検出結果の詳細に表示されます。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) 」を参照してください。

UnauthorizedAccess:EC2/MetadataDNSRebind

EC2 インスタンスが、インスタンスメタデータサービスに解決する DNS 検索を実行しています。

デフォルトの重要度: [High] (高)

- **データソース;** DNS ログ

この検出結果は、AWS 環境の EC2 インスタンスが、EC2 メタデータ IP アドレス (169.254.169.254) を決定するドメインをクエリしていることを知らせるものです。この種類の DNS クエリは、インスタンスが DNS リバイディング技術の対象であることを示している可能性があります。この手法は、インスタンスに関連付けらた IAM 認証情報など、EC2 インスタンスからメタデータを取得するために使用できます。

DNS リバインディングには、EC2 インスタンスで実行されているアプリケーションをだまして URL から返されるデータをロードすることが含まれます。URL のドメイン名は EC2 メタデータ IP アドレス (169.254.169.254) に解決されます。これにより、アプリケーションは EC2 メタデータにアクセスし、攻撃者がそのメタデータを使用できるようにする可能性があります。

EC2 インスタンスが URL の追加を許可する脆弱なアプリケーションを実行している場合や、EC2 インスタンスで実行されているウェブブラウザで、誰かが URL にアクセスする場合のみ、DNS リバインディングを使用して EC2 メタデータにアクセスできます。

修復のレコメンデーション

この検出結果に応じて、EC2 インスタンスで実行されている脆弱性アプリケーションがあるか、誰が検出結果で識別したドメインへアクセスするためブラウザを使用しているかを評価する必要があります。根本的な原因が脆弱なアプリケーションである場合は、脆弱性を修復する必要があります。ユーザーが識別したドメインを閲覧した場合、ドメインをブロックするか、ユーザーがそのドメインにアクセスできないようにします。この検出結果が上記のいずれかのケースに関連していると判断した場合は、EC2 インスタンスに関連付けられたセッションを取り消す必要があります (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_revoke-sessions.html) 。

一部の AWS のお客様は、メタデータ IP アドレスを信頼できる DNS サーバーのドメイン名に意図的にマッピングします。ご利用の環境でこのような状況が発生した場合は、この検出結果に対する抑制ルールを設定することをお勧めします。抑制ルールは、2 つのフィルター条件で構成する必要があります。1 つ目の条件では、**[Finding type]** (結果タイプ) 属性に

UnauthorizedAccess:EC2/MetaDataDNSRebind という値を使用します。2 つ目のフィルター条件では、**DNS リクエストのドメイン**を使用します。値はメタデータの IP アドレス (169.254.169.254) にマッピングしたドメインと一致する必要があります。抑制ルールの作成の詳細については、「抑制ルール (./findings_suppression-rule.html) 」を参照してください。

UnauthorizedAccess:EC2/RDPBruteForce

EC2 インスタンスが RDP ブルートフォース攻撃に巻き込まれています。

デフォルトの重要度: [Low] (低)*

> **注記**
>
> EC2 インスタンスが総当たり攻撃の対象である場合、この検出結果の重要度は「低」です。EC2 インスタンスが総当たり攻撃の動作主体である場合、この検出結果の重要度は「高」です。

- **データソース:** VPC フローログ

この検出結果は、 AWS 環境の EC2 インスタンスが、Windows ベースのシステムで RDP サービスへのパスワードを取得することを目的としたブルートフォース攻撃に関与していることを知らせるものです。これは、AWS リソースへの未承認のアクセスを示している場合があります。

修復のレコメンデーション

インスタンスの**リソースロール**が ACTOR の場合は、インスタンスが RDP 総当たり攻撃の実行に利用されたことを示しています。このインスタンスに Target としてリストされた IP アドレスと通信する合理的な理由がない限りは、インスタンスが侵害されたと仮定し、侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) でリストされたアクションを取ることをお勧めします。

インスタンスの **[Resource Role]** (リソースロール) が TARGET である場合は、セキュリティグループ、ACL、ファイアウォールのいずれかを使用して RDP ポートを信頼できる IP のみ保護することで、この検出結果を修復できます。詳細については、「EC2 インスタンスの保護のヒント (Linux)

(https://aws.amazon.com/articles/tips-for-securing-your-ec2-instance/) 」を参照してください。

UnauthorizedAccess:EC2/SSHBruteForce

EC2 インスタンスが SSH ブルートフォース攻撃に巻き込まれています。

デフォルトの重要度: [Low] (低)*

> **注記**
>
> 総当たり攻撃が EC2 インスタンスのいずれかを標的にしている場合、この検出結果の重要度は「低」です。EC2 インスタンスが総当たり攻撃の動作主体である場合、この検出結果の重要度は「高」です。

- **データソース:** VPC フローログ

この検出結果は、AWS 環境の EC2 インスタンスが、Linux ベースのシステムで SSH サービスへのパスワードを取得目的の総当たり攻撃に関与したことを知らせるものです。これは、AWS リソースへの未承認のアクセスを示している場合があります。

> **注記**
>
> この検出結果は、ポート 22 のモニタリングトラフィックを通じてのみ生成されます。SSH サービスが他のポートを使用するように設定されている場合には、この検出結果は生成されません。

修復のレコメンデーション

総当たり攻撃の対象が要塞ホストである場合、これはご利用の AWS 環境の想定内の動作を示している可能性があります。このような状況が発生した場合は、この検出結果に対する抑制ルールを設定することをお勧めします。抑制ルールは、2 つのフィルター条件で構成する必要があります。1 つ目の条件では、**[Finding type]** (結果タイプ) 属性に `UnauthorizedAccess:EC2/SSHBruteForce` という値を使用します。2 番目のフィルター条件は、要塞ホストとして機能する 1 つ以上のインスタンスと一致する必要があります。これらのツールをホストするインスタンスで識別可

能な条件に応じて、**[Instance image ID]** (インスタンスイメージ ID) 属性または **[Tag]** (タグ) 値の属性のいずれかを使用できます。抑制ルールの作成の詳細については、「抑制ルール (./findings_suppression-rule.html) 」を参照してください。

このアクティビティがご利用の環境で想定外であり、インスタンスの **[Resource Role]** (リソースロール) が `TARGET` である場合は、セキュリティグループ、ACL、ファイアウォールのいずれかを使用して SSH ポートを信頼できる IP のみ保護することで、この検出結果を修復できます。詳細については、「EC2 インスタンスの保護のヒント (Linux) (https://aws.amazon.com/articles/tips-for-securing-your-ec2-instance/) 」を参照してください。

インスタンスの **[Resource Role]** (リソースロール) が `ACTOR` の場合は、インスタンスが SSH 総当たり攻撃の実行に利用されたことを示しています。このインスタンスに `Target` としてリストされた IP アドレスと通信する合理的な理由がない限りは、インスタンスが侵害されたと仮定し、侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html) でリストされたアクションを取ることをお勧めします。

UnauthorizedAccess:EC2/TorClient

EC2 インスタンスが Tor Guard または Authority ノードに接続しています。

デフォルトの重要度: [High] (高)

- **データソース:** VPC フローログ

この検出結果は、AWS 環境の EC2 インスタンスが TorGuard または 権限ノードに接続中であることを知らせるものです。Tor は匿名通信を有効化するソフトウェアです。Tor Guards および Authority ノードは、Tor ネットワークへの初期ゲートウェイとして動作します。このトラフィックは、この EC2 インスタンスが侵害され、Tor ネットワーク上のクライアントとして動作していることを示している場合があります。この検出結果は、攻撃者が真のアイデンティティを隠して、AWS リソースへの不正アクセスを示している場合があります。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon

EC2 インスタンスの修復 (./compromised-ec2.html)」を参照してください。

UnauthorizedAccess:EC2/TorRelay

EC2 インスタンスが Tor リレーとして Tor ネットワークに接続しています。

デフォルトの重要度: [High] (高)

- **データソース:** VPC フローログ

この検出結果は、AWS 環境の EC2 インスタンスが Tor リレーとして動作していることを示す方法で、Tor ネットワークに接続中であることを知らせるものです。Tor は匿名通信を有効化するソフトウェアです。ある Tor リレーから別の Tor リレーにクライアントの不正なトラフィックを転送することで、通信の匿名性を高めます。

修復のレコメンデーション

このアクティビティが予期しないものである場合、インスタンスは侵害されている可能性があります。詳細については、「侵害された可能性のある Amazon EC2 インスタンスの修復 (./compromised-ec2.html)」を参照してください。
