

Cloud Security Study

Baptiste HEHN - 2315755, Ilias BETTAYEB - 2092408, Benoit DAMBRINE - 2075984 ,
Hany BASSI - 1956554

December 11, 2023

Abstract

Le but de cette étude scientifique est d'étudier l'exploitation du cloud computing sur AWS. L'objectif principal est d'enquêter sur l'émergence et le lancement d'attaques de phishing liées au spam par courrier électronique à l'aide des instances AWS EC2. L'objectif est de mettre en évidence les risques associés à ces activités malveillantes et de fournir une preuve de concept montrant comment les attaquants peuvent exploiter les ressources du cloud pour collecter des informations sensibles. Il sera par la suite possible d'héberger la page de phishing sur la même instance. Il est important de noter que cette étude constitue une preuve de concept et donne un aperçu des risques associés au cloud computing non autorisé sur AWS. Cette portée évite intentionnellement d'entrer dans les détails techniques complexes de la mise en œuvre de l'attaque, car l'objectif principal est de démontrer la simplicité et la faisabilité de la fraude. Pour pouvoir réaliser cette étude, il était d'abord important de configurer correctement l'infrastructure. La conclusion la plus importante de cette étude est que une page de phishing peut être mise en place simplement. Les attaquants peuvent utiliser des outils simples et facilement accessibles pour accéder à des informations sensibles, pénétrer dans des système ou infecter l'ordinateur d'un usager sans les autorisations appropriées. Nos recherches montrent que la facilité de ces attaques conduit à une utilisation accrue du cloud à des fins de phishing

1 Introduction

1.1 Contexte

L'importance de la sécurité du cloud dans les environnements de cloud computing modernes s'est accrue à mesure que les entreprises utilisent de plus en plus les services cloud pour améliorer leur efficacité, leur flexibilité et leur évolutivité. La sécurité du cloud est cruciale pour protéger les actifs numériques et les informations sensibles contre les différents risques du cloud computing.

Les principes, méthodes et technologies qui composent la sécurité du cloud sont utilisés pour contrôler et protéger les environnements cloud. Des systèmes conformes, des contrôles d'accès stricts et des normes internationales font partie de l'ensemble. Le respect de ces normes améliore la sécurité et garantit la conformité aux exigences réglementaires mondiales. L'adoption d'un cloud sécurisé offre de nombreux avantages, tels qu'une flexibilité organisationnelle accrue, une sécurité des données améliorée et des capacités améliorées de reprise après sinistre. Un niveau de sécurité plus élevé est atteint par le fournisseur de cloud, qui maintient les systèmes avec des correctifs et des mesures de sécurité à jour et permet des licences évolutives.

Le cloud computing présente plusieurs avantages, mais sa vulnérabilité aux erreurs de configuration et aux cyberattaques met en évidence la nécessité d'une sécurité dans le cloud.

1.2 Énoncé du Problème

Dans le cloud computing contemporain, en particulier sur des plateformes comme Amazon Web Services (AWS), un défi important et complexe apparaît : la menace croissante d'une utilisation abusive par des entités malveillantes. Cette étude vise à dévoiler les subtilités et les défis spécifiques liés au cloud computing abusif sur AWS, en mettant l'accent sur l'un des vecteurs d'attaque cloud courants utilisés par les acteurs de la cybercriminalité pour exploiter les capacités des fournisseurs de services cloud.

Les fournisseurs de services cloud, dont AWS, jouent un rôle central dans les opérations informatiques des entreprises, en proposant des solutions évolutives, flexibles et rentables. Cependant, les mêmes attributs qui rendent les services cloud attrayants pour les entreprises en font également des cibles attrayantes pour les acteurs malveillants cherchant à compromettre les environnements d'entreprise. À mesure que de plus en plus d'entreprises adoptent des approches multicloud et cloud hybride, le risque d'utilisation abusive du cloud à des fins malveillantes devient de plus en plus prononcé.

Les attaques par déni de service distribué (DDoS) constituent le principal vecteur utilisé par les acteurs malveillants. En surchargeant les serveurs Web, les systèmes ou les réseaux avec du trafic, les attaquants perturbent l'accès des utilisateurs légitimes, exploitant souvent des comptes cloud piratés ou des essais utilisateur gratuits pour ces attaques. Les conséquences sont graves, entraînant une indisponibilité du service et des pertes financières potentielles pour les entreprises qui dépendent d'AWS pour leurs opérations.

Les tentatives de phishing représentent un autre vecteur répandu d'utilisation abusive des ressources cloud. Les cybercriminels exploitent les techniques de phishing pour voler les informations d'identification des utilisateurs des services cloud, permettant ainsi un accès non autorisé et facilitant divers schémas malveillants.

Le spam par courrier électronique, un défi permanent en matière de cybersécurité, prend une nouvelle dimension lorsqu'il est orchestré via une infrastruc-

ture cloud. Les spammeurs utilisent la fiabilité et la bande passante des services cloud pour distribuer des messages électroniques en masse, en tirant parti des capacités de l'infrastructure.

Le cryptojacking, un ajout relativement récent à la gamme de cybermenaces, est également utilisé dans l'utilisation abusive d'AWS. Les attaquants accèdent aux ressources cloud d'une organisation et exploitent ces actifs pour des opérations d'extraction de cryptomonnaie, en utilisant la puissance de calcul de la victime.

Les services cloud compromis servent également de plateforme pour héberger du contenu malveillant. Des pages de phishing aux robots spammeurs, les attaquants utilisent l'infrastructure pour dissimuler le contenu nuisible aux côtés du matériel légitime, ce qui rend la détection plus difficile.

Comprendre ces vecteurs d'attaque cloud courants est essentiel pour développer des stratégies et des contre-mesures efficaces afin d'atténuer l'utilisation abusive des services cloud sur des plateformes comme AWS. Alors que les entreprises évoluent dans le paysage complexe du cloud computing, il devient primordial de sécuriser leurs environnements cloud contre ces tactiques en évolution.

1.3 Étendue de l'Étude

Cette étude vise à enquêter sur l'utilisation abusive du cloud computing sur AWS. L'objectif principal est d'explorer la génération et le lancement d'attaques de phishing accompagnées de spam par courrier électronique, à l'aide des instances AWS EC2. L'intention est d'établir une preuve de concept, démontrant les risques associés à ces activités malveillantes et démontrant la facilité avec laquelle les attaquants peuvent exploiter les ressources du cloud pour collecter des informations confidentielles. Il sera par la suite possible d'héberger la page d'hameçonnage avec cette même instance.

Cependant, certains éléments ne seront pas considérés dans cette étude en raison de contraintes de ressources. Notamment, l'étude n'englobe pas le déploiement automatisé du spam par courrier électronique avec des instances EC2 supplémentaires.

De plus, les vecteurs d'attaque alternatifs, tels

que le cryptojacking ou les attaques par déni de service distribué, ne sont pas à l'étude. L'étude se concentre intentionnellement sur les attaques de phishing et le spam par courrier électronique afin de maintenir la clarté et de présenter efficacement les activités abusives ciblées. Les contraintes de ressources financières, rendent difficile l'exploration d'autres vecteurs d'attaque qui demandent davantage d'instances.

Il est essentiel de noter que cette étude constitue une preuve de concept, offrant un aperçu des risques associés au cloud computing abusif sur AWS. Le champ d'application évite délibérément d'entrer dans les détails techniques complexes de la mise en œuvre de l'attaque, car l'objectif principal est de démontrer la simplicité et la faisabilité d'activités abusives.

2 Travaux Connexes

La problématique de l'abus du cloud computing a suscité l'attention de la communauté de recherche, et plusieurs articles ont contribué à éclairer les divers aspects de cette question. Douze de ces articles ont été analysés dans le cadre de cette étude.

Le premier article explore les préoccupations des utilisateurs de services cloud liées à l'attribution potentielle d'adresses IP figurant sur une blacklist. Les découvertes majeures soulignent la nécessité de vérifications régulières à l'aide d'outils tels qu'IPVoid. Pour les fournisseurs de services cloud, la réaffectation rapide des adresses IP abusives pose des défis. Deux solutions sont proposées : la collecte d'IP dans les blacklists et des mesures à l'encontre des utilisateurs malveillants[3]. Le deuxième article met en avant la nécessité d'un système de réputation des utilisateurs et des machines virtuelles (VMs) pour optimiser la classification des alertes générées par les IDS dans le cloud à [6]. Cependant, cela soulève des préoccupations quant à l'impact sur la confidentialité des données. Le troisième article propose SM-CIDS, un système de détection d'intrusions personnalisé pour les clients cloud, soulignant l'importance d'une sélection judicieuse des règles en fonction des services cloud hébergés [8].

Les deux derniers articles convergent sur le con-

stat que les IDS dans le cloud génèrent un nombre considérable d'alertes. Le deuxième article préconise l'utilisation d'un système de réputation, tandis que le troisième insiste sur une sélection plus adaptée des règles en fonction des services. Le premier article s'applique concrètement à la découverte du deuxième en proposant un système de réputation par la mise en place de blacklists.

Le quatrième article aborde divers problèmes tels que le traitement de données, le hijacking du trafic, des APIs non sécurisées, des attaques de déni de service, des attaques internes et l'abus du cloud. Les chercheurs concluent que l'abus des infrastructures à des fins malveillantes est le problème de sécurité le moins étudié [10].

Le cinquième article souligne l'abondance de recherche dans le domaine de la sécurité infonuagique, mais note un manque spécifique de recherche sur l'abus des ressources infonuagiques, alignant sa conclusion sur celle du premier article [1].

Le sixième article, quant à lui, réitère le manque de recherche sur l'abus de l'infonuagique pour des cyberattaques. Il encourage une focalisation sur le développement d'outils sécurisant les plateformes infonuagiques de l'intérieur [2].

Les articles sept, huit et neuf convergent sur l'abus potentiel des services cloud pour lancer des attaques malveillantes. L'article huit propose des techniques proactives pour prévenir l'accès non autorisé aux informations sensibles stockées dans le cloud. L'article neuf met en évidence le modèle de responsabilité partagée des fournisseurs cloud, plaçant la responsabilité de la sécurité sur les utilisateurs. L'article dix souligne le besoin de renforcer les processus d'enregistrement pour prévenir les abus, tandis que l'article onze examine les mécanismes de distribution et d'évasion dans les attaques de cryptojacking [5] [4] [7].

L'article dix présente BitDeposit, un système utilisant Bitcoin pour dissuader les attaquants potentiels par le biais de dépôts [9].

La compilation et l'analyse des articles examinés ont offert une compréhension approfondie des divers vecteurs d'attaque liés à l'abus du cloud computing. Ces travaux ont éclairé les préoccupations des utilisateurs, les défis rencontrés par les fournisseurs de

services cloud, ainsi que les lacunes en matière de sécurité et de sensibilisation.

3 Methodologie

3.1 Réponse aux Incidents

La réponse aux incidents dans le cloud englobe des aspects clés tels que la gouvernance, la responsabilité partagée et la visibilité, qui la différencient des systèmes traditionnels. Une planification de la réponse aux incidents est nécessaire dans le contexte des incidents cloud.

Un facteur important contribuant à ces différences est le modèle de responsabilité partagée mis en œuvre par les fournisseurs de services cloud. De plus, les différents modèles de services, notamment l'infrastructure en tant que service et le logiciel en tant que service, nécessitent des stratégies de réponse personnalisées.

Les incidents dans le cloud peuvent se manifester sous diverses formes, allant d'un accès non autorisé aux données et de mauvaises configurations à des informations d'identification compromises et des violations à grande échelle entraînant une perte de données. La diversité des incidents potentiels nécessite une stratégie de réponse aux incidents flexible et adaptative.

3.2 Plan de Réponse aux Incidents

Un plan de réponse aux incidents est essentiel pour une défense rapide contre les compromissions, les menaces internes et les abus d'accès dans les environnements AWS. Un confinement rapide et une réponse efficace sont essentiels pour atténuer les dommages et préserver la réputation. Les considérations spécifiques à AWS dans le plan de réponse aux incidents doivent tenir compte de l'architecture cloud unique, du modèle de responsabilité partagée et des diverses offres de services afin de garantir une stratégie de réponse adaptée et efficace.

3.3 Détection des Incidents et Rapports

Dans l'environnement AWS, des outils tels qu'AWS Security Hub, Amazon EventBridge et Incident Manager peuvent être utilisés en synergie pour une analyse solide des incidents de sécurité. En configurant les règles EventBridge liées aux résultats de Security Hub, les incidents sont automatiquement générés. De plus, il est essentiel de configurer la journalisation des services et des applications pour conserver les journaux d'événements de sécurité à des fins d'audit, d'enquête et à des fins opérationnelles, conformément aux normes de gouvernance et de conformité. L'analyse centralisée des journaux, des résultats et des mesures est cruciale pour les opérations de sécurité. Même si les outils de recherche aident à identifier les incidents potentiels, le traitement manuel devient peu pratique en raison de la complexité des architectures AWS. L'analyse et le reporting automatisés sont impératifs pour attribuer rapidement des ressources afin de répondre efficacement aux événements de sécurité.

La détection des incidents de sécurité implique la surveillance des modifications de configuration inattendues et des comportements inhabituels. Lors du déploiement de la charge de travail, les contrôles de configuration à l'aide d'AWS natifs ou d'outils tiers garantissent le respect des principes de sécurité. La surveillance continue détecte les changements inattendus après le déploiement. Des outils tels qu'Amazon GuardDuty identifient les activités non autorisées et la surveillance des appels d'API en mutation permet de maintenir la sécurité. Un examen régulier des mécanismes de détection est crucial pour la conformité. Les alertes automatisées, basées sur des conditions définies, facilitent une enquête rapide. Les canaux de signalement des vulnérabilités suspectées incluent le contact avec aws-security@amazon.com pour les services AWS ou les projets open source, en utilisant PGP pour une communication sécurisée. Les clients AWS peuvent effectuer des évaluations de sécurité sans approbation préalable pour des services spécifiés et signaler les abus à abuse@amazonaws.com. Les demandes liées à la conformité peuvent être adressées

via AWS Artifact. Pour les problèmes de sécurité d'Amazon.com, une page Web dédiée traite de divers problèmes, notamment les commandes suspectes ou les vulnérabilités.

3.4 Confinement

Lors de la détection d'un incident, une action rapide est cruciale pour le confinement dans un environnement cloud. Cela implique d'isoler les instances affectées, d'ajuster temporairement les règles du groupe de sécurité ou de désactiver les comptes d'utilisateurs compromis. Les stratégies de confinement dépendent de facteurs tels que les dommages potentiels, la préservation des preuves et la disponibilité des services.

3.5 Éradication et Rétablissement

L'éradication, partie intégrante de la réponse aux incidents, implique l'élimination des ressources suspectes ou non autorisées pour restaurer un compte dans un état sûr connu. Conformément au NIST SP 800-61, les étapes comprennent l'identification et l'atténuation des vulnérabilités exploitées, la suppression des logiciels malveillants et la répétition de la détection et de l'analyse pour les hôtes nouvellement affectés. Dans AWS, l'utilisation de journaux et d'outils tels que CloudWatch Logs et GuardDuty affine l'éradication. Les actions impliquent l'identification d'actions IAM non autorisées, de modifications d'accès, de création de ressources ou de modifications du système. Après l'identification, évaluez l'impact sur l'entreprise, puis effectuez une rotation ou supprimez des clés, des informations d'identification et des ressources. Les examens de sécurité, les analyses de vulnérabilités et le respect des politiques de sécurité garantissent une éradication efficace conforme aux besoins de l'organisation.

3.6 Analyse des Journaux

L'analyse des données de journaux est cruciale pour comprendre les activités des utilisateurs, les appels d'API et les modifications des ressources dans les

services cloud. Avec des outils tels que CloudWatch Logs Insights, il est possible de rechercher et analyser efficacement les journaux, facilitant ainsi la réponse aux incidents. Cet outil fournit un langage de requête spécialement conçu, des exemples de requêtes pour divers journaux de service AWS et la possibilité d'utiliser le langage naturel pour la génération de requêtes. Les requêtes dans CloudWatch Logs Insights peuvent être enregistrées, permettant la réutilisation de requêtes complexes sans les recréer. Il est essentiel de noter que ces requêtes peuvent entraîner des frais en fonction de la quantité de données interrogées, comme indiqué dans la tarification Amazon CloudWatch.

4 Methodology

4.1 Analyse des causes profondes (RCA)

Définition : L'analyse des causes profondes (Root Cause Analysis en anglais) est un processus d'identification des facteurs ou causes sous-jacents d'un problème ou d'un incident. Il s'agit d'une méthode structurée utilisée pour comprendre les principales raisons qui contribuent aux problèmes au sein d'un système.

Objectif : L'objectif principal de RCA est d'identifier les causes fondamentales des problèmes et/ou des incidents. Ceci permet aux organisations d'aller au-delà de la simple réponse aux incidents et s'attaquer aux véritables sources des problèmes.

Valeur ajoutée : L'approche d'analyses des causes profondes permet d'éviter la répétition de problèmes similaires à l'avenir. Cette analyse permet aussi l'allocation des ressources de manière plus efficace en orientant les efforts vers les problèmes fondamentaux. Enfin, elle contribue à l'atténuation des risques en identifiant de manière précise les problèmes systémiques qui pourraient présenter des risques pour la sécurité, la qualité ou d'autres aspects critiques des opérations. En ce faisant, le système voit sa résilience augmenter et devient plus optimisé.

Dans la section suivante, nous allons voir plus en détail les différentes causes profondes qui rentrent en

jeu dans le contexte de notre projet.

4.1.1 Accès à de puissantes ressources informatiques :

Cause : Les plates-formes cloud fournissent des ressources informatiques facilement accessibles et évolutives, tant en termes de puissance de calcul (vertical scaling) qu'en termes de nombre de ressources (horizontal scaling), permettant aux individus de déployer et de gérer une infrastructure complexe avec un minimum d'effort.

Implication : Cette accessibilité facilite le déploiement d'infrastructures de malicieuses, telles que celles du phishing dans notre contexte, avec la capacité de gérer un grand volume d'activités frauduleuses.

4.1.2 Anonymat:

Cause : Les services cloud offrent un niveau d'anonymat, permettant aux individus de créer et de gérer des ressources sans révéler leur véritable identité.

Implication : Les acteurs malveillants peuvent se cacher derrière l'anonymat fourni par les services cloud, ce qui rend difficile pour les autorités de les retrouver et d'engager des poursuites judiciaires à leur rencontre.

4.1.3 Disponibilité mondiale :

Cause : Les fournisseurs de cloud disposent de centres de données répartis dans le monde entier, permettant aux utilisateurs de déployer des ressources dans différents emplacements géographiques.

Implication : Des campagnes de phishing peuvent être lancées à l'échelle mondiale, ciblant les victimes dans diverses régions.

4.1.4 Abus de services légitimes :

Cause : Les plates-formes cloud offrent une variété de services légitimes qui peuvent être réutilisés pour des activités malveillantes, telles que les services de messagerie, l'hébergement Web et les réseaux de diffusion de contenu.

Implication : Les acteurs malveillants peuvent exploiter ces services légitimes pour héberger des sites Web de phishing, distribuer des e-mails de phishing ou diffuser du contenu malveillant. Cet abus peut passer inaperçu pendant de longues périodes.

4.1.5 Provisionnement automatisé :

Cause : Les environnements cloud encouragent le provisionnement automatisé. Ceci permet ainsi le déploiement et la gestion de l'infrastructure via le code.

Implication : L'infrastructure de phishing peut être provisionnée et détruite par programme, permettant aux attaquants d'agir rapidement et d'éviter les mécanismes de détection statiques. Cette nature dynamique pose des défis au niveau de la sécurité.

4.1.6 Pré-vérification limitée des utilisateurs :

Cause : Les fournisseurs de cloud donnent souvent la priorité à la commodité de l'utilisateur et peuvent avoir des processus de pré-vérification moins stricts que les fournisseurs d'hébergement traditionnels.

Implication : Les attaquants peuvent exploiter la facilité de création de compte avec une vérification minimale, ce qui simplifie la configuration et l'exploitation d'une infrastructure malveillante sans subir de contrôles d'identité rigoureux.

4.2 Recommandations suite au RCA:

- Les fournisseurs de services cloud devraient améliorer les procédures de vérification d'identité.
- Collaboration améliorée entre les fournisseurs de cloud et les forces de l'ordre pour une réponse plus rapide aux rapports d'abus.
- Sensibilisation et éducation renforcées à la sécurité pour aider les utilisateurs à identifier les tentatives de phishing.
- Surveillance et analyse continues des ressources cloud pour les activités anormales.

4.3 Récupération

La phase de récupération consiste à restaurer et à vérifier la fonctionnalité des systèmes concernés pour reprendre les opérations commerciales normales. Cela peut inclure des tâches telles que :

- Restauration à partir de sauvegardes : si les données ou les configurations ont été compromises, la restauration à partir de sauvegardes devient une étape cruciale dans la récupération du système.
- Reconstruction des ressources cloud : tirer parti des services cloud pour reconstruire tous les composants affectés lors de l'incident.
- Application des correctifs : mise en œuvre des correctifs ou des mises à jour nécessaires pour remédier aux vulnérabilités identifiées lors de la RCA.

4.4 Communication

La communication joue un rôle central après la RCA, soulignant l'importance d'examiner l'incident pour tirer des leçons et améliorer le processus de réponse aux incidents. Les aspects clés comprennent :

- Tirer les leçons des incidents : identifier les leçons tirées de l'incident, y compris les améliorations des processus, des procédures et les mises à jour potentielles des mesures de sécurité.
- Prévenir des événements similaires : décrire des stratégies et des mesures pour prévenir des incidents similaires à l'avenir sur la base des informations acquises grâce au RCA.
- Informer les parties prenantes : communiquer avec les diverses parties prenantes au sujet de l'incident. Fournir des informations précises et concises sur l'incident, son impact et les mesures prises pour le résoudre.

4.5 Durcissement post-incident

Le durcissement post-incident se concentre sur le renforcement de l'environnement cloud. Cela implique :

- Mise en œuvre de mesures de sécurité : Améliorer les mesures de sécurité en fonction des vulnérabilités et des faiblesses identifiées lors du RCA.
- Stratégies de confinement et d'atténuation : discuter des stratégies et des meilleures pratiques pour contenir et atténuer les incidents de sécurité.
- Restauration des services : détaillant les mesures prises pour restaurer les services et décrivant toutes les modifications apportées pour éviter des incidents similaires.

4.6 Défis

4.6.1 Modèle de responsabilité partagée :

Le modèle de responsabilité partagée implique de reconnaître et de relever les défis liés à la répartition des responsabilités entre le fournisseur de services cloud et l'organisation. Il faut clarifier les responsabilités en garantissant une compréhension claire des responsabilités du fournisseur de services cloud et de l'organisation en matière de mesures de sécurité.

4.6.2 Complexité et échelle :

La gestion de la complexité et de l'échelle des environnements cloud présente des défis uniques. Elle implique la mise en œuvre de mesures de sécurité adaptatives capables de répondre de manière dynamique à la nature changeante et à la portée étendue de ces activités malveillantes. Cela peut inclure l'exploitation de la détection avancée des menaces telle que la détection d'anomalies par apprentissage automatique.

4.6.3 Forensique:

Bien que dans ce rapport, nous n'allons pas rentrer en détail sur ce point, il reste nécessaire d'effectuer

la réalisation d'analyses judiciaires pour comprendre la portée et l'impact des incidents. Après avoir effectué l'analyse des causes profondes (RCA) pour identifier les raisons sous-jacentes de l'incident, il est impératif de procéder à une analyse forensique pour une compréhension plus complète et des considérations juridiques potentielles.

L'analyse forensique implique la collecte, la préservation et l'examen des preuves pour mieux comprendre l'incident, notamment la chronologie des événements, l'étendue de la compromission et l'impact potentiel. Ce processus englobe la collecte de données, la reconstruction de la chronologie et des techniques d'analyse telles que l'analyse de la mémoire, l'investigation des disques et l'investigation des réseaux.

La documentation des conclusions forensiques dans un rapport détaillé est cruciale. La réalisation d'une analyse forensique à la suite d'un incident garantit une compréhension approfondie, facilite la conformité légale et améliore la préparation aux futurs incidents de sécurité.

4.7 Services et composants cloud

Services AWS formant le cœur de l'infrastructure :

4.7.1 VPC (Virtual Private Cloud) :

Brève explication : Fournit un réseau virtuel pour les ressources dans AWS. Il offre une isolation logique et un contrôle total sur l'environnement réseau.

4.7.2 Instance EC2 :

Brève explication : L'instance EC2 représente un serveur virtuel dans le cloud. C'est un élément fondamental permettant d'exécuter des applications sur l'infrastructure d'AWS.

4.7.3 Table de routage :

Brève explication : La table de routage gère le cheminement du trafic à l'intérieur du VPC. Elle détermine comment le trafic est dirigé entre les différentes ressources au sein du réseau.

4.7.4 Passerelle Internet :

Brève explication : La passerelle Internet facilite la communication entre les instances du VPC et Internet. Elle permet aux ressources dans le VPC d'accéder à des services en ligne et d'être accessibles depuis Internet.

4.7.5 ACL réseau (liste de contrôle d'accès) :

Brève explication : L'ACL réseau agit comme un pare-feu au niveau du sous-réseau, contrôlant le trafic entrant et sortant. Elle offre une couche de sécurité supplémentaire en définissant des règles d'accès.

4.7.6 Groupe de sécurité :

Brève explication : Le groupe de sécurité agit comme un pare-feu virtuel pour une instance EC2, contrôlant le trafic réseau. Il spécifie les règles d'accès entrant et sortant pour garantir la sécurité.

4.7.7 Sous-réseau :

Brève explication : Le sous-réseau représente une plage d'adresses IP dans notre VPC. Il permet de segmenter le réseau en fonction des besoins et d'appliquer des règles spécifiques à chaque sous-réseau.

4.7.8 Association de tables de routage :

Brève explication : L'association de tables de routage lie un sous-réseau à une table de routage spécifique. Cela permet de définir les règles de routage spécifiques à chaque sous-réseau, contribuant ainsi à une gestion flexible du trafic au sein du VPC.

4.8 Configuration de l'infrastructure

4.8.1 Configuration VPC (vpc.tf) :

- **Bloc CIDR :** "10.100.0.0/16"
- **Support DNS :** Activé
- **Noms d'hôtes DNS :** Activé
- **Tags :** Nom : "gophish-vpc"

4.8.2 Configuration de l'instance EC2 (ec2.tf) :

- **AMI** : "ami-087c17d1fe0178315" (Amazon Linux 2)
- **Type d'instance** : "t2.micro"
- **Paire de clés** : Référencé à partir de la ressource AWS Key Pair
- **Subnet** : Référencé à partir de la ressource de sous-réseau AWS
- **Groupes de sécurité** : Référencé à partir de la ressource AWS Security Group
- **User Data**: Exécute un script pour configurer Gophish et MailHog.

4.8.3 Configuration de la table de routage (routes.tf) :

- **Association VPC** : Associé au VPC spécifié.
- **Route par défaut** : Achemine le trafic (0.0.0.0/0) vers la passerelle Internet.

4.8.4 Configuration de la passerelle Internet (igw.tf) :

- **Association VPC** : Associé au VPC spécifié.
- **Tags** : Nom : "gophish-igw"

4.8.5 Configuration de l'ACL réseau (nacl.tf) :

- **Ingress Rule** : Autorise tout le trafic entrant (0.0.0.0/0).
- **Egress Rule** : Autorise tout le trafic sortant (0.0.0.0/0).

4.8.6 Configuration du groupe de sécurité (security_groups.tf) :

- **Règles d'entrée** :
 - SSH (Port 22)

- HTTP (Port 80)
- Serveur Gophish (Port 3333)
- Accès MailHog (Port 8025)

- **Egress Rule** : Autorise tout le trafic sortant (0.0.0.0/0).

4.8.7 Configuration du sous-réseau (subnets.tf) :

- **Bloc CIDR** : "10.100.10.0/24"
- **Mappage IP public** : Activé
- **Zone de disponibilité** : "us-east-1a"
- **Tags** : Nom : "public-subnet-67354a08"

4.8.8 Configuration d'association de table de routage (associations.tf) :

- **Subnet Association** : Associé au sous-réseau public spécifié.
- **Association de table de routage** : Associé à la table de routage spécifiée.

4.9 Surveillance et journalisation

4.9.1 Configuration :

Configuration de la surveillance :

- Nous avons opté pour l'utilisation d'AWS CloudWatch pour surveiller la consommation de ressources telles que le CPU, la mémoire, et d'autres métriques essentielles. Cette configuration nous permet de visualiser en temps réel les performances de nos instances EC2, de définir des alertes personnalisées et d'agir en cas de variations anormales.

4.9.2 Journalisation centralisée :

Configuration de la journalisation :

- Pour centraliser la journalisation des événements, nous avons mis en place AWS CloudWatch Logs. Cette solution nous permet de collecter, stocker et analyser de manière centralisée les journaux générés par nos instances EC2. Des filtres et des métriques personnalisés sont également configurés pour faciliter l'identification rapide d'événements clés.

Pour la détection d'anomalies, bien que nous n'ayons pas encore intégré de solution basée sur l'IA, notre approche repose sur l'analyse régulière des métriques CloudWatch, en particulier la surveillance attentive de la consommation CPU, de la mémoire et d'autres ressources pertinentes. Ces analyses manuelles nous permettent d'identifier des tendances inhabituelles ou des pics de charge, anticipant ainsi les éventuels problèmes de performances. Il serait pertinent dans un travail futur d'également d'explorer des solutions basées sur l'IA, telles qu'Amazon CloudWatch Anomaly Detection, pour renforcer la capacité à détecter automatiquement les anomalies dans les métriques critiques.

5 Experiments

5.1 Mise en place du Proof of Concept

Pour notre projet final, comme précisé auparavant, nous avons décidé de réaliser un Proof of Concept afin de montrer la simplicité de la mise en place d'une campagne de phishing en utilisant le Cloud. Nous avons tout d'abord eu l'idée de mettre en place une infrastructure (voir figure 1) contenant :

- 1 VPC contenant les différents éléments qui sont exposés à internet via une Gateway.
- 1 instance EC2 pour héberger la page de landing du phishing et également le client Gophish pour réaliser les campagnes de phishing.
- 1 serveur AWS SES (Simple Email Service), qui est un serveur smtp pour l'envoi des emails de phishing.

- 1 réservation de nom de Domaine avec AWS route 53 afin de rendre la landing page de notre campagne de phishing plus crédible.

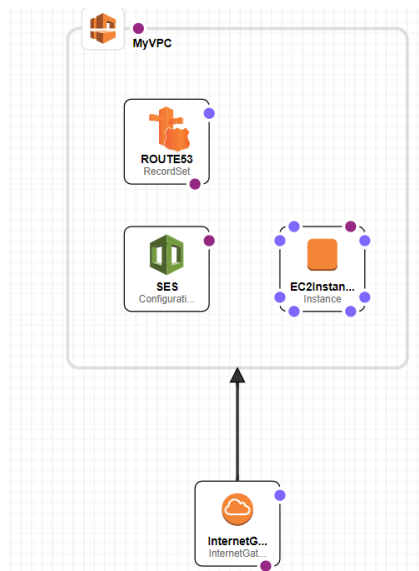


Figure 1: Figure de l'architecture initiale

Cependant, nous sommes limités par les autorisations du rôle laboratoire d'AWS, et nous n'avons pas accès au service SES et route 53. Nous avons donc décidé de restreindre notre Proof of Concept à une infrastructure plus limitée :

- 1 VPC que nous avons pu mettre en place avec l'exposition à internet via l'inter Gateway,
- 1 instance EC2 pour l'hébergement de la campagne de phishing

Après avoir mis en place l'architecture, il nous faut utiliser l'outil Gophish. Nous avons décidé d'utiliser le smtp de polytechnique pour réaliser des campagnes de phishing sur nos propres mails poly face aux limitations exprimées auparavant. Avec Gophish, nous avons réalisé plusieurs template permettant de copier un email du registraire de poly et d'usurper l'identité du registraire. On peut ensuite modifier les liens contenus dans ce mail pour rediriger la victime vers notre instance EC2 où l'on héberge une landing page

copiée à partir du vrai dossier étudiant de poly et ainsi récupérer les credentials. De plus, on peut choisir de rediriger l'utilisateur vers le vrai dossier étudiant après qu'il a rempli et envoyé ses credentials afin qu'il ne se doute de rien. Gophish propose également un suivi de chaque campagne de phishing réalisé permettant de savoir le nombre d'emails envoyés, le nombre d'emails ouvert, le nombre de victimes ayant cliqué sur les liens malicieux et le nombre de victimes ayant envoyé leur credentials. Des images de gophish présentant les différentes parties de la configuration sont disponibles dans la partie Annexes.

6 Experiments (Continued)

6.1 Proof of Concept

L'objectif principal du Proof of Concept que nous avons décidé de mettre en place, est de montrer que le déploiement via des scripts Terraform ou encore Cloud Formation permet via le Cloud de facilement réaliser des campagnes de phishing en déployant toutes les ressources nécessaires en quelques minutes. En effet, les points les plus complexes de la mise en place de la campagne de phishing sont, l'hébergement de la landing page, la mise en place d'un serveur smtp et la réservation d'un nom de domaine. Or, tous ces points sont facilités par l'usage du Cloud, les Cloud providers nous fournissant des services visant à faciliter ces processus.

6.2 Infrastructure Penetration Testing

6.2.1 Objective

- L'objectif d'un test de pénétration est d'identifier les vulnérabilités dans les environnements cloud. Dans le cadre de notre projet final, un test de pénétration n'a pas réellement d'intérêt, mais on pourrait également penser à associer une attaque par des individus malveillants pour installer un client Gophish et utiliser une instance légitime pour héberger une campagne de phishing.

6.2.2 VPC Peering Attacks

- Tout d'abord, il convient de rappeler ce qu'est le VPC peering. Dans AWS, il est possible de permettre à deux réseaux virtuels privés de communiquer entre eux de manière sécurisée, c'est le VPC peering. Cependant, des attaques sont possibles sur cette fonctionnalité.
- L'une des attaques les plus courantes est le VPC hijacking. Cette attaque désigne le fait qu'un individu malveillant, réussi à compromettre les informations nécessaires pour la mise en place du VPC peering. L'attaquant a donc accès aux ressources de l'autre VPC auquel il est désormais connecté. La vulnérabilité la plus courante et importante est une mauvaise configuration des rôles IAM. Par exemple, un non-respect du principe de moindre privilège permettrait un accès au VPC peering à un rôle qui ne devrait pas y avoir accès. De plus, une mauvaise gestion de la création et destruction des connexions du VPC peering avec les rôles IAM, est aussi une autre vulnérabilité importante.

6.2.3 EC2 Instance Breach

- Nous avons imaginé et mis en place un scénario afin de gagner l'accès à une instance EC2 afin d'y installer un client Gophish et pouvoir ensuite réaliser des campagnes de phishing :
 - Ce scénario serait une configuration IAM et des comptes de l'instance EC2 permettant à un compte de maintenance de faire des installations sur l'instance et d'avoir des privilèges équivalents aux privilèges root ou administrateur. De plus, la connexion ssh à l'instance se fait via mot de passe et non clé asymétriques, ce qui rend la connexion par un individu extérieur plus simple. Également, le mot de passe du compte de cette instance n'est pas un mot de passe très compliqué, car il est partagé entre plusieurs personnes et il est utilisé quotidiennement. En effet, après avoir réalisé une campagne de spear phishing sur les personnes ayant

accès à ce compte, l'attaquant récupère le mot de passe "123456" pour se connecter au compte maintenance. Il réussit à s'y connecter et obtient des privilèges beaucoup trop important pour un compte de maintenance. Il ne reste plus qu'à l'attaquant d'installer le client Gophish avec les privilèges du compte maintenance, et il peut lancer des campagnes de phishing à partir de cette instance.

6.3 Test de Détection d'Anomalie

6.3.1 Objectif

L'objectif lors de la détection d'anomalie dans le cloud est de trouver des anomalies du comportement du cloud qui indiquerait entre autre un comportement malveillant. Dans le cas de l'abus du cloud, la détection d'anomalie comportementale permet de reconnaître une situation où un compte AWS est utilisé à des fins d'abus. Pour effectuer une détection efficace, il est nécessaire d'avoir un comportement normal d'un compte cloud pour ensuite pouvoir le comparer à un comportement malveillant. Des metriques utilisées pour évaluer le comportement d'un compte sont le trafic réseau et les appels API au compte AWS. L'analyse de métrique n'est pas suffisant pour la detection d'activité malveillante. Il est donc nécessaire d'instaurer l'utilisation d'outils de détection d'utilisation malveillante du cloud. Un outil interne de AWS existent déjà, GuardDuty. Cet outil permet de réduire l'utilisation abusive du cloud pour des actions malveillantes. En plus, de devoir détecter l'abus dans le cloud, il est essentiel d'utiliser des outils permettant de détecter le phishing. Ces outils devraient être basés dans une infrastructure cloud.

6.3.2 Augmentation Trafique Réseau

Lors de notre expérimentation, il est évident que l'utilisation du réseau augmente. Les instances qui heberge un site de phishing vont évidemment voir une hausse de trafic, ce qui est normal dans le contexte d'une campagne de phishing. Par contre,

cette hausse serait considérée normale pour une instance hébergeant un site non malveillant. Il est donc difficile de baser notre détection d'instance malveillante sur une augmentation soudaine du trafic d'un réseau. De plus, lors d'une campagne de phishing utilisant les infrastructure du cloud, il est peu probable qu'un des site de phishing voit le trafic réseau augmenter de façon suspect. Se baser sur des augmentations soudaine de trafic réseau n'est donc pas une metrique utiles pour la détection d'abus du cloud pour des campagne de phishing.

6.3.3 Appels d'API AWS suspicieux

Concernant les appels suspicieux de l'API AWS, ils ne diffèrent pas particulièrement d'une instance qui n'effectue pas d'activités de phishing. Il est donc difficile de se baser sur les appels d'API pour définir un comportement s'éloignant du comportement normal. Par contre dans le contexte où un acteur malveillant, prend contrôle d'une instance, il est pertinent d'évaluer les appels d'API suspicieux. En effet, lorsqu'un mauvais acteur prend le contrôle d'une instance des appels suspicieux d'API AWS pourraient être fait. Il serait donc important d'évaluer si les appels d'API sont suspects et non habituels.

6.3.4 Déclenchement d'Alertes GuardDuty

GuardDuty est l'outil le plus utile pour la détection d'abus du cloud pour effectuer des campagne de phishing. Cet outil permet de monitorer un compte AWS pour des activités malicieuses. Il se base sur les logs pour détecter des comportements divergeant du comportement considéré normale. Il permet aussi à l'utilisateur de rester informé sur toutes actions suspicieuses qui se déroule dans son compte pour pouvoir y remédier. Dans le cas de l'utilisation du cloud pour effectuer hebergé des sites de phishing, Guard Duty détecte plusieurs activités suspicieuses, un type évident est EC2/UnusualDNSResolver. Ce type de déviation d'un comportement déviant de la baseline démontrerait possiblement une attaque de phishing effectuée au sein du compte AWS. De plus, si un attaque prend le contrôle de notre instance pour effectuer des attaques de type phishing, GuardDuty

reconnait d'autre type d'activités suspectes. Il reconnaît toutes les activités liées au Backdoor, car notre instance communiquerait avec des adresses IPs non sécurisés. Les activités suspectes de type DefenseEvasion seraient aussi reconnues.

6.4 Évaluation de l'Efficacité de la Surveillance

6.4.1 Objective

La performance de la génération de log dans AWS est très bonne. Les logs sont très détaillés et permettent une compréhension profonde de nos instances. La granularité des métriques dans AWS est très bonne. Il y a plusieurs options pour granulariser les métriques. On peut changer la période sur laquelle on veut voir les métriques, on peut changer la répétition de l'évaluation permettant une grande granularité. Finalement, AWS fournit un très bon système pour stocker et récupérer les logs. Ces logs peuvent être en quantité astronomique, mais AWS fournit un système simple et efficace pour gérer cette énorme quantité de données.

6.4.2 Latence de Génération de Log

Le temps de génération d'un log est presque nul. Il est essentiel pour un système moderne d'avoir la génération de log presque instantanée, pour la surveillance dynamique du système. Il est nécessaire de réagir instantanément et pour cela il faut pouvoir évaluer les logs de façon instantané. Le système doit être à jour avec toutes les activités qui se produisent pour pouvoir réagir instantanément, donc un système de log sans délai est obligatoire.

6.4.3 Test de Granularité des Métriques

Il est essentiel d'avoir des métriques avec une grande granularité. Dans le cas d'AWS, les métriques ont très grande granularité ce qui permet d'examiner en détails les données collectées par le système d'analyse de métrique d'AWS. Cet analyse permet d'assurer une compréhension profonde de notre système et

des activités de sécurité. Cette grande granularité apportée par AWS permet d'être efficace dans l'identification d'événement de sécurité.

6.4.4 Stockage et Récupération de Log

Le système de stockage et de récupération de logs dans AWS est efficace. Il permet de rapidement trouver des logs, malgré la quantité énorme qu'une seule instance produit. Il est essentiel d'avoir un bon système de stockage de logs, pour les analyses post-mortem. Il faut donc tester régulièrement le système de stockage, car des pertes de logs peuvent être un grave problème future. Le système de récupération doit être aussi très performant, car lors d'analyse il faut pouvoir rapidement avoir accès à des logs spécifiques.

7 Discussion

7.1 Trouvailles clés

Notre trouvaille principale est la facilité avec laquelle un site de phishing est implémentable. Avec des outils simples et facilement accessibles, un mauvais acteur peut réussir à obtenir des informations sensibles d'un usager, rentrer dans des systèmes sans les droits appropriés ou infecter l'ordinateur de quelqu'un. On remarque dans notre étude que la facilité que ces attaques entraînent une augmentation de l'abus du cloud pour effectuer du phishing. Les attaquants utilisent des infrastructures cloud, dans notre cas AWS, car le cloud permet de la mise à l'échelle horizontale et verticale. Ces avantages sont utiles pour des utilisateurs normaux, mais sont utilisés de façon néfaste par des utilisateurs malveillants pour améliorer leurs attaques. Il est donc évidemment nécessaire d'améliorer les solutions de sécurité. Un autre aspect qu'on a découvert lors de notre travail est la flexibilité qu'apporte AWS et le cloud en général lors de campagne de phishing. Cette flexibilité permet à l'attaquant de créer et de détruire des sites de phishing rapidement. Il peut changer l'adresse IP ou le contenu de la page très rapidement comparé à une infrastructure on site. Ce qui rajoute un couche de difficulté lors de la détection et la prévention de

ce type d'attaque. Notre travail démontre la facilité qu'un mauvais acteur peut effectuer une attaque de type phishing avec l'infrastructure cloud, il est donc essentiel pour les industries cloud et les spécialistes de la sécurité cloud de se pencher sur ce problème.

7.2 Limitations

Lors de notre projet et particulièrement notre proof of concept, nous avons fait face à trois limitations principales. La première est que nous avons un compte amazon web service étudiant. Donc nous étions limité sur le nombre d'instance que nous pouvions déployer en même temps. De plus ce type de compte ne permet pas certaines activités, ce qui nous a empêché de pousser notre proof of concept plus loin. Les deux autres limitations sont liées au type de compte que nous avons. La première concerne la création d'un serveur SMTP. Nous voulions utiliser le Simple Email Service (SES) qu'un compte normal AWS fournit. Ce service nous aurait permis de créer notre propre serveur SMTP est donc d'envoyer des courriels avec des fausses adresses courriels de notre choix. Nous nous sommes tournés vers le serveur SMTP de l'école Polytechnique Montréal, considérant son manque de sécurité, il était simple d'envoyer un courriel avec l'adresse courriel de n'importe qui. La deuxième limitation concerne l'utilisation du service Route 53, qui permet d'associer une URL à notre adresse ip public de notre instance. Ce service n'est pas inclus dans le type de compte étudiant et demande des frais supplémentaire. Nous avons donc décidé de ne pas utiliser d'adresse URL, pour notre proof of concept. Dans le cas d'un vrai phishing, il est nécessaire d'avoir une URL associée aux adresses des sites vulnérables. Ces trois vulnérabilités, ne nous a pas empêcher de faire un proof of concept permettant de conclure de la facilité et de l'efficacité que l'abus du cloud pour des sites de phishing permet.

7.3 Implications

L'étude de l'abus du cloud particulièrement la création de campagne de phishing avec celui-ci est un type d'attaque qui évolue rapidement. Ce type

d'attaque peut être dévastateur pour un individu ou une entreprise. La facilité avec laquelle un mauvais acteur peut effectuer ces attaques et la difficulté de détecter ce type d'attaque démontrent l'importance de ce problème. Il est donc nécessaire qu'Amazon développe des mesures protectives et que les entreprises se rendent compte de la valeur de leurs informations.

8 Conclusion et travail futur

8.1 Conclusion

Lors de notre projet, nous vous avons présenter les différentes menaces de sécurité que le cloud présentent. En particulier, nous nous sommes concentrés sur l'aspect de l'abus du cloud qui est un sujet de cybersécurité qui est peu recherché. Nous avons commencé par présenter le contexte dans lequel notre projet à lieu. Ensuite nous avons énoncé notre problématique en expliquant les différentes possibilités d'abus du cloud et nous avons présenté l'étendue de l'étude. Nous avons fait une analyse des travaux connexes sur lesquelles nous nous sommes basés pour faire le projet. À la section 3, la méthodologie lors d'un incident de sécurité et la réponse aux incidents est présentée. Ensuite à la section 4, l'analyse des causes profondes est présentée. Plusieurs causes sont présentées avec leurs implications par rapport à notre sujet, par exemple, l'accès à de puissantes ressources informatiques et l'anonymat venant avec un compte AWS. À la suite des causes, il y a plusieurs sections rajoutant de diverses explications sur la procédure après l'analyse des causes. Finalement les sections 4.7 à 4.9 présentent les différents aspects méthodologique de l'infrastructure cloud AWS. Les sections 5 et 6 présentent la mise en place du proof of concept et le proof of concept en soi. Finalement, la section 7 permet de discuter des trouvailles clés, des limitations et des implications de notre projet.

8.2 Recommendations

En ce qui concerne les recommandations suite à notre projet, il est évident pour une organisation

de sensibiliser les employés au courriel suspicieux, au lien suspicieux dans les courriels et aux fichiers suspicieux dans les courriels. Un mauvais acteur peut facilement déployer et détruire des instances permettant du phishing, la vigilance aux attaques de phishing est essentielle. L'utilisation de firewall bien mis en place permet une bonne protection contre ce type d'attaque.

8.3 Travail Future

Notre projet a mis en lumière le manque flagrant d'outil efficace permettant la détection d'activité d'abus au sein du cloud. Il est donc primordial d'avancer la recherche dans cette direction. Nous pensons qu'il faut développer des meilleurs outils utilisant la technologie du machine learning pour détecter des activités d'abus au sein du cloud et particulièrement détecter des attaques de type phishing effectué dans le cloud. De plus, le développement d'outils utilisant le cloud pour détecter des attaques phishing, en analysant les URLs ou les courriels. Des outils hébergés dans le cloud de type machine learning qui permettraient de réduire le succès de ces attaques. Un dernier aspect où la recherche devrait se pencher est la détection du phishing dans le fog et le edge computing. Ces technologies évoluent rapidement et doivent être sécurisées. Il faut donc étudier rapidement ces nouvelles technologies et les sécuriser.

9 Acknowledgements

Nous aimerions remercier Alex Rodriguez et Jim Lamb dont les articles sur Medium.com nous ont permis d'installer des attaques de phishing rapidement et efficacement. De plus nous aimerions remercier puzzlepeaches sur GitHub sur lequel nous nous sommes basés pour faire notre Dockerfile.

10 Annexes

11 References

References

- [1] Ishrat Ahmad and Humayun Bakht. "Security challenges from abuse of cloud service threat". In: *International Journal of Computing and Digital Systems* 8.01 (2019), pp. 19–31.
- [2] Moitrayee Chatterjee et al. "Abuse of the Cloud as an Attack Platform". In: *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE. 2020, pp. 1091–1092.
- [3] Naoki Fukushi et al. "A large-scale analysis of cloud service abuse". In: *2020 IEEE Conference on Communications and Network Security (CNS)*. IEEE. 2020, pp. 1–9.
- [4] Yasir Ahmed Hamza and Marwan Dahar Omar. "Cloud computing security: abuse and nefarious use of cloud computing". In: *Int. J. Comput. Eng. Res* 3.6 (2013), pp. 22–27.
- [5] Geng Hong et al. "How you get shot in the back: A systematical study about cryptojacking in the real world". In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. 2018, pp. 1701–1713.
- [6] Jens Lindemann. "Towards abuse detection and prevention in IaaS cloud computing". In: *2015 10th International Conference on Availability, Reliability and Security*. IEEE. 2015, pp. 211–217.
- [7] Kashif Munir. *Handbook of research on security considerations in Cloud Computing*. IGI Global, 2015.
- [8] Seyed Mostafa Siadat, Mojtaba Rezvani, and Hossein Shirgahi. "Proposing a secure method for intrusion detection in Amazon EC2 public cloud". In: *Researchgate. Net*, no. January (2016).

Edit Template

Name:

test_tmplate

 Import Email

Envelope Sender: ?

registraire@polymtl.ca

Subject:

Paiement des frais de scolarité

Text

HTML

```
<html>
<head>
  <title></title>
</head>
<body>
<p>&lt;html xmlns:v=&quot;urn:schemas-microsoft-com:vml&quot; xmlns:o=&quot;
urn:schemas-microsoft-com:office:office&quot; xmlns:w=&quot;urn:schemas-microsoft-
```

Figure 2: Email template Gophish

Edit Sending Profile



Name:

sending_profile

Interface Type:

SMTP

SMTP From: ?

registraire@polymtl.ca

Host:

smtp.polymtl.ca:587

Figure 3: Smtplib configuration Gophish

New Campaign ×

Name:

test_projet_final

Email Template:

test_tmplate

Landing Page:

test_landing_page

URL: ?

http://3.223.140.15

Launch Date

December 4th 2023, 1:53 am

Send Emails By (Optional) ?

Sending Profile:

sending_profile

✉ Send Test Email

Groups:

× test_gn

Close

✈ Launch Campaign

Figure 4: Campagne Gophish

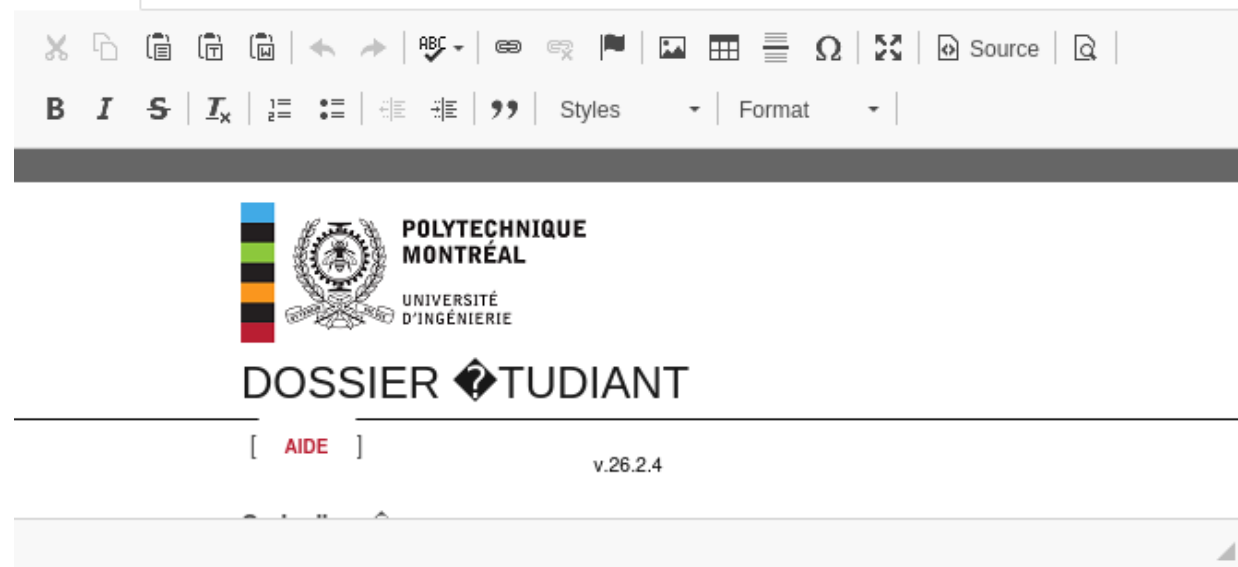
New Landing Page ×

Name:

test_landing_page

 Import Site

HTML



☐ Capture Submitted Data 

Cancel

Save Page

Figure 5: Landing page Gophish

Results for test_projet_final

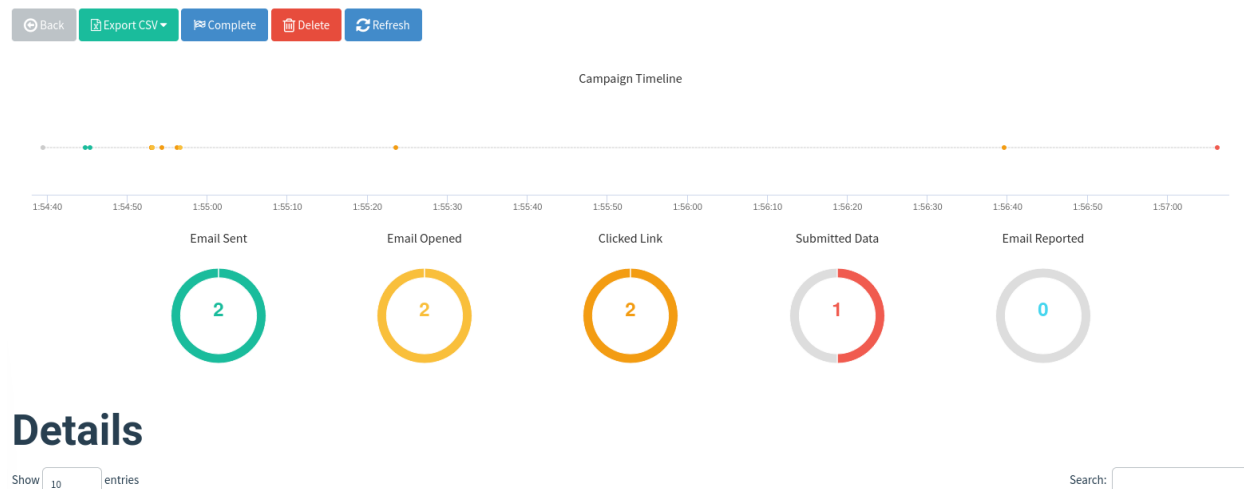


Figure 6: Récapitulatif campagne Gophish

- [9] Jakub Szefer and Ruby B Lee. “Bitdeposit: Detering attacks and abuses of cloud computing services through economic measures”. In: *2013 13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing*. IEEE. 2013, pp. 630–635.
- [10] Dinesh Taneja and SS Tyagi. “Information Security in cloud computing: A Systematic Literature Review and analysis”. In: *International Journal of Scientific Engineering and Technology* 6.1 (2017), pp. 50–55.