Université de Technologie d’Haïti (UNITECH)

Banque de la République d’Haïti (BRH)

***Sécurité des Systèmes Informatiques (SSI)***

Sujet

***« Analyse de l'attaque par ransomware Ryuk contre PEMEX (Mexique, 2019) »***

Sous la direction du Professeur

Blaise ARBOUET

Présenté par le groupe 4

Jean Lukens DERILUS

Joël ALEXIS

Joseph Jeff FORESTAL

Luckens JEAN

26 Mai 2025

**TABLE DES MATIERES**

[**1.** **Introduction** 2](#_Toc198937944)

[**2.** **Sommaire exécutif** 3](#_Toc198937945)

**3. Chronologie de l'ataque………………………………………………...…………………………4**

[**4.** **Contexte** 5](#_Toc198937946)

[**4.1** **Présentation de PEMEX** 5](#_Toc198937947)

[**4.2** **Portée de l’attaque** 6](#_Toc198937948)

[**5.** **Enjeux de cybersécurité** 7](#_Toc198937949)

[**5.1** **Vulnérabilité des infrastructures critiques** 7](#_Toc198937950)

* 1. [**Conséquences économiques et politiques ………………………………………………..…...**7](#_Toc198937950)

[**5.3** **Conséquences politiques ………………………………………………………………………9**](#_Toc198937950)

[**5.4** **Transformation des menaces** 9](#_Toc198937951)

[**6.** **Classification des données** 10](#_Toc198937952)

[**6.1** **Types de données concernées** 10](#_Toc198937953)

[**6.2** **Sensibilité et classification** 10](#_Toc198937954)

[**6.3** **Impact potentiel sur la sécurité des données** 11](#_Toc198937955)

[**7.** **Analyse de risque** 12](#_Toc198937956)

[**7.1** **Identification des menaces** 12](#_Toc198937957)

[**7.2** **Vulnérabilités exploitées** 12](#_Toc198937958)

[**7.3** **Evaluation de l’impact** 12](#_Toc198937959)

[**8.** **Recommandations** 13](#_Toc198937960)

[**8.1** **Mesures préventives** 13](#_Toc198937961)

[**8.2** **Mesures détectives** 13](#_Toc198937962)

[**8.3** **Mesures correctives** 13](#_Toc198937963)

[**8.4** **Cadres et bonnes pratiques** 13](#_Toc198937964)

[**9.** **Conclusion** 14](#_Toc198937965)

[**10.** **Bibliographie** 15](#_Toc198937966)

1. **Introduction**

La cybersécurité est devenue une priorité stratégique pour les organisations, en particulier celles opérant dans des secteurs critiques comme l'énergie. Avec l'augmentation constante des cybermenaces, les entreprises doivent faire face à des attaques de plus en plus sophistiquées, souvent motivées par des gains financiers ou des objectifs de déstabilisation. L’attaque par ransomware contre Petróleos Mexicanos (PEMEX), la compagnie pétrolière nationale du Mexique, en novembre 2019, illustre bien les risques auxquels les infrastructures critiques sont exposées.

Cette attaque, attribuée au ransomware Ryuk, a provoqué une interruption temporaire des systèmes de gestion de l’entreprise, affectant certains processus opérationnels. Les auteurs de l’attaque ont exigé une rançon de cinq millions de dollars pour restaurer l’accès aux données chiffrées. Si PEMEX a officiellement refusé de payer la rançon, l’incident a mis en lumière les failles potentielles de sécurité dans des systèmes aussi sensibles que ceux d’une entreprise énergétique d’envergure nationale.

L’objectif de ce rapport est d’analyser l’incident de cybersécurité subi par PEMEX, d’en examiner les enjeux techniques et organisationnels, et de proposer des recommandations concrètes pour améliorer la posture de cybersécurité de ce type d’organisation. Ce travail s’inscrit dans le cadre d’une réflexion plus large sur la protection des infrastructures critiques en Amérique Latine, région de plus en plus ciblée par les cybercriminels.

1. **Sommaire exécutif**

**Contexte et Périmètre de l’attaque**

Entre 9 et 11 novembre 2019, Petróleos Mexicanos (PEMEX) a été la cible d’une cyberattaque par ransomware (Ryuk/DoppelPaymer) qui a chiffré ses systèmes administratifs et de facturation, perturbant et paralysant la gestion des paiements et des communications internes.

**Type attaque**

Ransomware (chiffrement des données)

**Acteur identifie**

Ryuk

**Date**

Début d’attaque ; 9 novembre 2019, publication ; 11 novembre 2019

**Montant demande**

565 BTC (Bitcoins) équivalent à presque 5M USD

**Vulnérabilité – Résumé**

Intrusion initiale via une campagne de phishing ou une porte dérobée permettant ainsi au malware de se propager latéralement.

**Impact principal constate**

Disponibilité : 5% des ressources informatiques, serveurs et postes ont été affectés entrainant une indisponibilité des systèmes de facturation, gestion des fournisseurs, de messagerie, obligeant les équipes à effectuer le traitement manuel des opérations.

Intégrité / Confidentialité : Chiffrement des données sensibles paralysant les processus internes et certains services administratifs (Facturation, gestion des communications internes, comptabilité etc…).

**Niveau de criticité / gravité**

Criticité : Critique, perte de disponibilité des services administratifs d’une infrastructure énergétique nationale, avec risque élevé pour la continuité des activités et la crédibilité institutionnelle.

Gravité : élevée, vue la position stratégique de PEMEX et des risques de perturbation de la chaine d’approvisionnement énergétique.

**Mesures recommandées**

1. Isolation immédiate et restauration depuis sauvegardes saines.
2. Segmentation stricte du réseau pour briser la propagation latérale.
3. Mise en oeuvre d’une politique de sauvegarde robuste.
4. Renforcement des controles d’accès et sensibilization/formation par rapport aux menaces (phishing).
5. Application rigoureuse des mises a jour.
6. Deploiement de solutions de detection d’intrusion.
7. Monitoring de manière continue (logs et activités reseaux).
8. Elaboration et test régulier d’un plan de réponse aux incidents.
9. Coordination avec les autorités nationales.
10. Adoption de référentiels internationaux (NIST Cybersecurity Framework, ISO 27001/27002 et CIS Controls).

**Plan de remediation**

1. Activation du plan de response, analyses forensic, sauvegarde isolees.
2. Restauration des services critiques.
3. Deploiment des correctifs et audit de sécurité.
4. Exercice complet de reprise et revue post-incident.
5. **Chronologie de l’attaque**

Selon Milenio, les premières attaques ont commencé le samedi 9 novembre. Le lendemain, des rumeurs circulaient sur les réseaux sociaux concernant une possible attaque par ransomware. Le lundi 11 novembre, le Secrétariat à l'Énergie du Mexique a tenté de calmer les esprits en précisant qu’il n’y aurait pas de pénurie d’essence. Le même jour, PEMEX confirmait la cyberattaque, tout en relativisant sa portée. La compagnie pétrolière affirmait que l’attaque n’a touché que 5% de ses équipements informatiques personnels et que la production, l'approvisionnement et les stocks de carburant étaient garantis. Ce n’est que 24 heures plus tard que les cybercriminels ont exigé l’équivalent de 5 millions de dollars en bitcoins pour déchiffrer les fichiers piratés. Entre-temps, le gouvernement mexicain a ouvert une enquête afin de déterminer si le personnel de PEMEX avait participé à la cyberattaque.

**Chronologie**

* **Intrusion initiale (avant le 10 novembre 2019)**
* Les attaquants auraient pu accéder au réseau via une campagne de phishing ou une vulnérabilité non corrigée.
* **Dimanche 10 novembre 2019 – Déploiement du ransomware**
  + Déploiement du ransomware sur les serveurs critiques.
  + Chiffrement des données sur plusieurs serveurs et postes de travail.
  + Affichage de messages de rançon exigeant un paiement (en bitcoin), sous menace de perte définitive des données.
  + PEMEX indique dans un communiqué que ces tentatives ont été « neutralisées », affectant néanmoins moins de 5 % de son parc informatique.
* **Lundi 11 novembre 2019 – Détection et première communication**
  + Blocage de l’accès à des fichiers et systèmes internes.
  + Dysfonctionnements majeurs dans les activités administratives.
  + Communication interne chaotique. Des courriels commencent à circuler en interne évoquant un **incident de cybersécurité**.
  + Le gouvernement (Secrétariat à l’Énergie) rassure le public : « pas de pénurie d’essence ».
  + Confirmation officielle de la cyberattaque. PEMEX rassurant que la production, l’approvisionnement et les stocks restent garantis.
* **Mardi 12 novembre 2019 – Exigence de rançon et refus**
* Réclamation de 565 BTC environ 5M $ pour le déchiffrement des données sensibles, avec une échéance au 30 novembre 2019.
* Les autorités mexicaines et PEMEX annoncent qu’ils ne céderont pas au chantage.
* **11–15 novembre 2019 – Réponse et remédiation**
* Mise en œuvre du plan d’urgence : isolation des systèmes infectés, restauration à partir de sauvegardes saines, et sauvegarde manuelle des données critiques.
* Lancement d’une enquête forensic et ouverture d’une investigation gouvernementale pour déterminer d’éventuelles complicités internes.
* Instruction aux employés de **ne pas allumer leurs ordinateurs**.
* Demande de **déconnexion du réseau**.
* Sauvegarde des données critiques sur **disques durs externes**.
* **Fin novembre 2019 – Renforcement et retour à la normale**
* Déploiement de correctifs, renforcement de la segmentation réseau et mise à jour des endpoints.
* Exercice de reprise après sinistre et renforcement des procédures anti-phishing et de surveillance en temps réel.

1. **Contexte**
   1. **Présentation de PEMEX**

**Petróleos Mexicanos (PEMEX)** est l’entreprise publique nationale du Mexique en charge de l’exploration, de la production, du raffinage et de la commercialisation du pétrole et du gaz naturel. Fondée en 1938, elle constitue l’un des piliers économiques du pays, représentant une source importante de revenus pour l’État mexicain. En raison de son rôle stratégique, PEMEX est considérée comme une **infrastructure critique nationale**, au même titre que les secteurs de la santé, des télécommunications ou de l’électricité.

L’entreprise gère un large réseau de raffineries, de terminaux, de pipelines et de systèmes d'information industriels (ICS/SCADA), nécessaires au fonctionnement de l'ensemble de la chaîne de production et de distribution de l'énergie.

PEMEX déclare dans un communiqué de presse que la cyberattaque de la veille avait été « ***neutralisée*** » dans les meilleurs délais. Plusieurs serveurs de PEMEX dans le monde impacté.

Moins de 5% de ses ordinateurs impactés. 5% de combien de milliers de machines ?

La multinationale ajoute espérer une solution dans les 48 heures. Elle conseille aux utilisateurs de ne pas allumer leurs ordinateurs. PEMEX demande aux employés de se déconnecter de son réseau. De sauvegarder les informations critiques à partir de disques durs.

* 1. **Portée de l’attaque**

L’attaque par ransomware s’est produite le **lundi 11** **novembre 2019 (**reconnue officiellement**)**, affectant spécifiquement les **systèmes de gestion internes** de l’entreprise. Bien que les opérations critiques de production n’aient pas été paralysées selon les autorités mexicaines, plusieurs départements ont vu leur activité ralentie, notamment en ce qui concerne la **facturation, la comptabilité et les communications internes**. Des messages d’erreur ont été signalés sur les ordinateurs des employés, indiquant une infection par le malware **Ryuk**.

Selon plusieurs rapports de cybersécurité, l’infection aurait été déclenchée à travers un **accès distant mal sécurisé (Remote Desktop Protocol - RDP)**, combiné à une campagne de phishing ciblée. Ce vecteur est fréquemment utilisé par les groupes cybercriminels affiliés à Ryuk pour compromettre les réseaux d'entreprise.

* 1. **Sources d'information**

Les informations sur cette attaque proviennent de diverses sources :

* Communiqués de presse officiels de PEMEX et du gouvernement mexicain ;
* Rapports techniques publiés par des entreprises de cybersécurité (Kaspersky, Symantec, etc.) ;
* Analyses d’experts indépendants et articles dans la presse spécialisée ;
* Données publiées sur les forums et dark web par les auteurs de Ryuk (dans certains cas, les groupes publient des données volées pour faire pression).

Ces éléments permettent de dresser un cadre précis de l’attaque, bien qu’une partie des données reste confidentielle, comme souvent dans les affaires de cybersécurité impliquant des infrastructures critiques.

1. **Enjeux de cybersécurité**
   1. **Vulnérabilité des infrastructures critiques**

L’attaque contre PEMEX met en lumière la **vulnérabilité des infrastructures critiques** face aux cybermenaces modernes. Les entreprises du secteur énergétique, comme PEMEX, exploitent des réseaux industriels complexes où coexistent des systèmes anciens (legacy systems) et des technologies récentes. Ces environnements hybrides sont particulièrement difficiles à sécuriser, d’autant plus que les impératifs de continuité de service limitent parfois les possibilités d’interventions techniques (mises à jour, audits, etc.).

La paralysie même partielle d’une entreprise comme PEMEX peut provoquer des **répercussions à l’échelle nationale**, affectant la production énergétique, les transports, les chaînes logistiques et, in fine, l’économie mexicaine.

* 1. **Conséquences économiques et politiques**

L’attaque par le ransomware **Ryuk** a eu des impacts économiques significatifs sur **PEMEX**, une entreprise stratégique pour l’économie mexicaine :

* **Interruption des activités administratives :**

L’indisponibilité temporaire des systèmes informatiques a entraîné une **paralysie des opérations internes**, notamment la gestion des contrats, la facturation, les paiements et les communications internes. Cette perturbation a affecté la chaîne logistique et les partenaires commerciaux.

* **Coûts de remédiation élevés :**

Bien que PEMEX ait affirmé ne pas avoir payé la rançon, l’entreprise a dû mobiliser des ressources importantes pour :

* + L’identification des vecteurs d’attaque,
  + La **restauration des systèmes**,
  + La **mise à niveau de la cybersécurité**,
  + La **formation des employés** sur les bonnes pratiques numériques.

Ces coûts incluent l'intervention de spécialistes en cybersécurité et l’acquisition de nouveaux outils de protection, engendrant **des pertes financières directes et indirectes**.

* **Atteinte à la réputation :**

L’incident a fragilisé l’image de PEMEX sur les marchés financiers et auprès de ses partenaires internationaux, accentuant les doutes sur sa **capacité de gestion des risques numériques**.

* **Perturbation du marché énergétique :**

En tant qu'acteur clé du secteur énergétique mexicain, la vulnérabilité de PEMEX face aux cybermenaces a semé l’inquiétude chez les investisseurs et régulateurs. Bien que la production de pétrole n’ait pas été directement impactée, l’incident a souligné la dépendance critique aux systèmes numériques dans les infrastructures pétrolières.

#### **Conséquences politiques**

* **Pression sur le gouvernement mexicain :**

En tant qu’entreprise publique, PEMEX est sous la responsabilité de l’État. L’attaque a généré **une vive pression politique** sur le gouvernement de l’époque, l’obligeant à répondre aux critiques concernant :

* + le **niveau de préparation du pays face aux cyberattaques**,
  + la **cybersécurité des institutions stratégiques**.
* **Renforcement de la législation :**

L’incident a accéléré les discussions autour de la **mise en place d’une stratégie nationale de cybersécurité** au Mexique. Il a également contribué à l’élaboration de politiques publiques visant à protéger les infrastructures critiques.

* **Instrumentalisation politique :**

Certains partis d’opposition ont utilisé l’attaque comme argument pour dénoncer la gestion jugée déficiente de l’entreprise par le gouvernement en place, en particulier en ce qui concerne les **investissements technologiques** et la **modernisation de PEMEX**.

* 1. **Transformation des menaces**

Le cas PEMEX illustre aussi une **évolution des cybermenaces** : les ransomwares ne se contentent plus de bloquer des ordinateurs individuels, mais visent désormais des réseaux entiers. Des groupes comme ceux derrière Ryuk adoptent une approche dite de **“big-game hunting”**, ciblant les grandes entreprises et exigeant des rançons très élevées.

Les attaques sont de plus en plus :

* **Ciblées** (reconnaissance préalable, privilèges élevés),
* **Discrètes** (infiltration lente),
* **Destructrices** (chiffrement massif, parfois vol de données en amont), rendant les méthodes classiques de protection partiellement obsolètes.

1. **Classification des données**
   1. **Types de données concernées**

L’attaque par ransomware Ryuk contre PEMEX a potentiellement affecté plusieurs catégories de données critiques, utilisées quotidiennement par l’entreprise :

* **Données opérationnelles** : informations relatives aux processus industriels, commandes, états des équipements, données SCADA (Supervisory Control and Data Acquisition).
* **Données financières** : facturation, budgets, comptes clients et fournisseurs.
* **Données RH** : informations personnelles des employés, contrats, paies.
* **Données stratégiques** : plans d’affaires, projets d’investissement, données sensibles liées à la sécurité nationale.
* **Données clients et partenaires** : contrats commerciaux, correspondances, rapports d’audit.
  1. **Sensibilité et classification**

Afin de mieux appréhender la criticité des données touchées, il est utile de les classifier selon la **triade CIA** (Confidentialité, Intégrité, Disponibilité) :

|  |  |  |  |
| --- | --- | --- | --- |
| Type de données | Confidentialité | Intégrité | Disponibilité |
| Données opérationnelles | Élevée | Élevée | Critique |
| Données financières | Élevée | Élevée | Haute |
| Données RH | Moyenne | Moyenne | Moyenne |
| Données stratégiques | Très élevée | Très élevée | Haute |
| Données clients/partenaires | Élevée | Élevée | Moyenne |

La disponibilité des données opérationnelles est particulièrement cruciale, car toute interruption peut entraîner une paralysie des processus industriels et une perte de contrôle sur les systèmes.

* 1. **Impact potentiel sur la sécurité des données**

Le chiffrement par ransomware Ryuk a pour effet principal de rendre les données indisponibles pour les utilisateurs légitimes, causant une perte d’accès temporaire ou prolongée. Toutefois, certains groupes exploitant Ryuk pratiquent aussi l’extorsion en menaçant de publier les données volées, ce qui augmente l’enjeu en matière de confidentialité.

Cette double menace impacte donc à la fois la **disponibilité** et la **confidentialité** des informations, avec un risque majeur pour la réputation et la compétitivité de l’entreprise.

1. **Analyse de risque**
   1. **Identification des menaces**

Le ransomware **Ryuk** est un logiciel malveillant ciblé utilisé principalement pour des attaques de type “big-game hunting” contre des grandes organisations. Il est souvent diffusé via des campagnes de phishing, des accès distants compromis (RDP non sécurisés) ou en tirant parti de vulnérabilités non corrigées.

Dans le cas de PEMEX, les experts estiment que l’attaque a exploité une combinaison de :

* Phishing ciblé auprès d’employés,
* Accès RDP mal sécurisé,
* Manque de segmentation du réseau,
* Absence de mises à jour critiques.
  1. **Vulnérabilités exploitées**
* **Accès distant non sécurisé** : un vecteur très courant dans les attaques Ryuk.
* **Faiblesse dans la segmentation réseau** : permettant une propagation rapide du ransomware dans l’environnement.
* **Absence ou insuffisance des sauvegardes** : qui empêche une restauration rapide.
* **Manque de surveillance et détection** : l’attaque a pu évoluer sans être détectée rapidement.
  1. **Evaluation de l’impact**
* **Interruption temporaire** de plusieurs services essentiels (facturation, communication).
* **Coûts financiers élevés** liés à la gestion de crise, la restauration et la perte de productivité.
* **Risque réputationnel** important au niveau national et international.
* **Menace sur la sécurité nationale** en cas de compromission des systèmes industriels.

1. **Recommandations**
   1. **Mesures préventives**

* **Renforcement des contrôles d’accès** : mise en place d’authentification multi-facteurs, restriction des accès RDP.
* **Sensibilisation et formation** des employés sur les risques de phishing.
* **Application rigoureuse des mises à jour** de sécurité pour les systèmes et logiciels.
* **Segmentation stricte du réseau** afin d’isoler les systèmes critiques.
  1. **Mesures détectives**
* Déploiement de solutions de **détection d’intrusion (IDS/IPS)** et de systèmes EDR (Endpoint Detection and Response).
* **Surveillance continue** des logs et activités réseau.
* Mise en place d’une **veille de menace** active sur les ransomwares et leurs variantes.
  1. **Mesures correctives**
* Élaboration et test régulier d’un **plan de réponse à incident**.
* Mise en œuvre d’une **politique de sauvegarde robuste**, incluant des copies hors ligne et hors site.
* Coordination avec les autorités nationales et les équipes CERT en cas d’incident.
  1. **Cadres et bonnes pratiques**

Adoption de référentiels internationaux comme :

* **NIST Cybersecurity Framework**,
* **ISO 27001** et **ISO 27002**,
* **CIS Controls** (Center for Internet Security).

1. **Conclusion**

L’attaque ransomware Ryuk contre PEMEX a révélé la **fragilité des infrastructures critiques face aux cybermenaces modernes**. Malgré une interruption temporaire des opérations, les répercussions économiques et stratégiques de cet incident sont un signal d’alarme pour l’ensemble des organisations similaires en Amérique Latine.

Pour renforcer la résilience face à ces menaces, il est impératif d’adopter une posture proactive intégrant prévention, détection et réponse rapide. La cybersécurité ne doit plus être une fonction isolée mais un enjeu transversal au sein des entreprises et des gouvernements.

La protection des infrastructures vitales, telles que les systèmes énergétiques, est également une responsabilité nationale, nécessitant une collaboration étroite entre les secteurs public et privé.

1. **Bibliographie**

* Kaspersky. (2020). *Ryuk Ransomware: What You Need to Know*.
* Symantec Security Response. (2019). *Ransomware Trends and Analysis*.
* NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*.
* ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.
* Reuters. (2019). *PEMEX hit by ransomware attack; company denies payment*.