



UNIVERSITÉ
DE TECHNOLOGIE D'HAÏTI



PROGRAMME TIC-HAÏTI-BRH

5/26/2025

Université de Technologie d'Haïti

UNITECH

DESS

Cours : Sécurité des Systèmes Informatiques

Groupe 7

- Lubens LUMA
- Renel SIDRENICE
- Wideline TAVIL
- Egzael LABADY
- John-Eder Exumé

Sujet : Le Piratage de Banco de Chile

Plan de la présentation

1. Objectif et méthodologie
2. Contexte de Banco de Chile
3. Chronologie de l'attaque
4. Nature et déroulement de l'attaque
5. Classification des données ciblées ou compromises
6. Effets de l'incident
7. Enjeux de cybersécurité (Confidentialité, Intégrité, Disponibilité)
8. Vulnérabilités et risques
9. Réponses institutionnelles (internes, gouvernementales, réglementaires)
10. Leçons stratégiques pour Haïti
11. Recommandations concrètes
12. Concepts vus en cours (ISO 27001, ISO 27005, IAAA, SIEM, PCA/PRA...)
13. Conclusion et ouverture
14. Références

Objectif et méthodologie

□ Objectif du travail

- Analyser un incident réel de cybersécurité majeur en Amérique Latine
- Identifier les vulnérabilités techniques, humaines et organisationnelles exploitées
- Proposer des recommandations concrètes et applicables au contexte haïtien
- Relier l'étude de cas aux concepts théoriques abordés dans le cours (SSI1024)

□ Méthodologie suivie

- Revue documentaire (rapports, articles, sources spécialisées)
- Analyse chronologique de l'attaque de Banco de Chile (2018)
- Évaluation des impacts : techniques, économiques, réputationnels
- Mise en lien avec les normes ISO/IEC 27001 & 27005 et les modèles vus en cours
- Élaboration de recommandations pour les institutions financières haïtiennes



Banco de Chile : Un acteur majeur du secteur financier

- Fondée en 1893, l'une des plus anciennes banques d'Amérique latine
- Millions de clients, milliers d'employés, présence nationale étendue
- **Services** : comptes, prêts, investissements, services aux entreprises, e-banking
- **Rôle crucial** dans l'économie chilienne, impliquée dans les transactions nationales et internationales
- Une modernisation numérique rapide... mais aussi de nouveaux risques cyber



Une modernisation numérique rapide... mais aussi de nouveaux risques cyber

Classification des données ciblées ou compromises

☐ Types de données visées lors de l'attaque

- Données internes sensibles : comptes administratifs, configurations système, accès IT
- Données financières : relevés de transactions, mouvements de fonds, accès SWIFT
- Données clients : informations personnelles, numéros de comptes, historiques d'opération
- Données d'authentification : identifiants, mots de passe, certificats

☐ Gravité de la compromission

- Risques de fraude bancaire, de vol d'identité et de pertes massives
- Atteinte directe à la confidentialité, à l'intégrité et à la disponibilité
- Conséquences juridiques, réputationnelles et opérationnelles majeures

Chronologie de l'attaque

Mai-Juin 2018

24 mai 2018

Panne détectée
dans les agences et
services téléphoniques



Début juin 2018

Découverte de
transactions suspectes
dans SWIFT



11 juin 2018

Confirmation du vol de
10 millions de dollars,
transférés à Hong Kong



28 mai 2018

Identification d'un virus
sur les postes de travail

11 juin 2018

Confirmation du vol
de 10 millions de dollars,
transférés à Hong Kong

Nature et déroulement de l'attaque

Phase 1: Malware Wiper



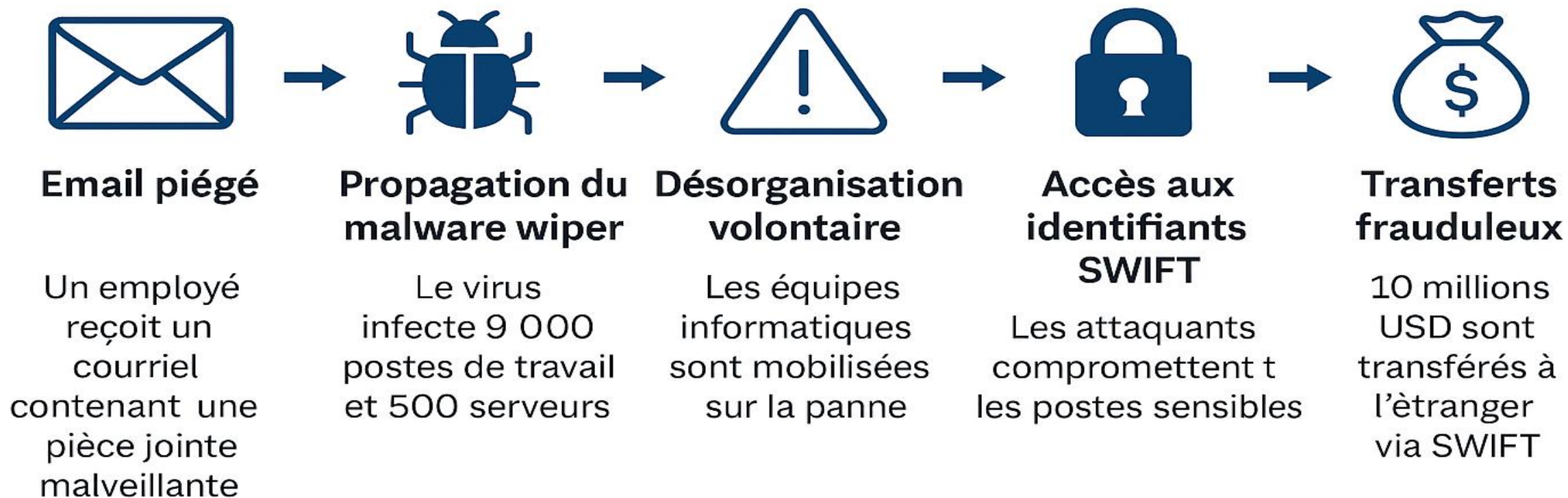
- Affectation de 9 000 PCs et 500 serveurs
- Désorganisation volontairement provoquée chez les équipes IT
- Exploitation du chaos pour agir sans interruption

Phase 2: Détournement via SWIFT

- Utilisation d'un SWIFT valide pour émettre une transaction
- Vol de 10 millions USD transférés vers des comptes en Asie
- Exploitation du chaos pour agir sans interruption

Une attaque planifiée, ciblée, discrète
et techniquement avancée.

Schéma du déroulement de l'attaque



Effets de l'attaque



Effets internes

- Paralysie de nombreux services informatiques
- Panne de 9 000 postes et 500 serveurs
- Interruption temporaire des opérations internes:
 - Comptabilité
 - Support client
 - Échanges interbancaires



Effets sur les clients

- Guichets automatiques (ATMs) hors service
- Plateformes en ligne inaccessibles (e-banking, virements)
- Augmentation des plaintes
- Perte de confiance des usagers et du grand public


▲ Une attaque visible, paralysante et fortement ressentie à tous les niveaux.

Enjeux de cybersécurité: le triangle CID




Ces trois piliers sont indispensables pour maintenir la confiance et la résilience des systèmes bancaires.

Vulnérabilités et risques

 **Risque** = Menace × Vulnérabilité × Impact

Exemples tirés de l'incident :

Menace	Vulnérabilité	Risque
Cybercriminels (APT)	Absence de segmentation réseau	Accès non autorisé à SWIFT via postes internes
Email piégé (phishing)	Mauvaise sensibilisation des utilisateurs	Infection initiale du réseau via malware wiper
Transactions SWIFT	Faible séparation des privilèges / pas d'audit	Vol de 10M USD sans détection immédiate

 Des vulnérabilités techniques et humaines ont facilité la matérialisation du risque.

Réponses institutionnelles



Mesures techniques immédiates:

- Isolement de segments réseau infectés
- Blocage d'accès à distance
- Désactivation temporaire du service SWIFT



Communication:

- Déclaration publique le 11 juin 2018
- Assurance donnée aux clients sur la non-affectation des comptes
- Coordination avec les autorités chiliennes et la banque centrale



Actions organisationnelles:

- Activation d'un plan de continuité d'activité (PCA)
- Renforcement de l'équipe cybersécurité
- Lancement d'un audit complet des systèmes

Leçons stratégiques pour Haïti

 Principaux enseignements de l'attaque de Banco de Chile :

- | | |
|---|--|
| <p>① Renforcer la gestion des accès
Implémenter le modèle IAAA
Séparation stricte des droits
(rôles, services, privilèges)</p> | <p>② Structurer la réponse
Élaborer un Plan de Continuité
(PCA) et un Plan de réponse
aux incidents</p> |
| <p> Former les utilisateurs
Sensibilisation au <i>phishing</i>
Réduction des erreurs humaines</p> | <p> Structurer la réponse
Élaborer un Plan de Continuité
(PCA) et un Plan de réponse
aux incidents</p> |

Haïti peut progresser malgré ses contraintes, avec une approche ciblée, réaliste et stratégique de la cybersécurité.

Recommandations concrètes



Techniques

- Segmenter le réseau (SWIFT, interne, DMZ...)
- Installer un SIEM open-source (ex: Wazuh)
- Activer la journalisation des logs critiques



Organisationnelles

- Mettre en place un PCA/PRA
- Définir une politique claire de gestion des accès
- Mettre en place un plan de réponse aux incidents



Humaines

- Sensibiliser contre le phishing
- Simuler des attaques pour tester l'équipe
- Former tous les nouveaux employés

✓ Des mesures *simples, efficaces et realistes* pour renforcer la cybersécurité sans exploser le budget.

Conclusion et Ouverture

Conclusion

- L'attaque contre Banco de Chile révèle la fragilité des systèmes bancaires connectés.
- Elle démontre la nécessité :
 - d'une gestion rigoureuse des accès
 - d'une préparation structurée
 - d'une cohérence entre technologie, organisation et formation

Ouverture

Et si demain, une banque haïtienne était ciblée ?

La question n'est plus si, mais quand.

Il est urgent de se préparer avec des moyens ciblés et une stratégie adaptée.

 **La cybersécurité ne se décrète pas : elle se construit, couche par couche, action après action.**

Références

Normes et cadres de sécurité :

- ISO/IEC 27001 – Système de management de la sécurité de l'information
- ISO/IEC 27005 – Gestion des risques liés à la sécurité de l'information

Notions du cours SSI1024 :

- Modèle IAAA (Identification, Authentification, Autorisation, Audit)
- Concepts clés : SIEM, PCA, PRA, RBAC, journalisation, analyse de risque
- Supports internes du cours (séances, documents, exercices)

Sources documentaires :

- Banco de Chile – Rapport officiel, 2018
- ThreatPost – Banco de Chile Confirms SWIFT Attack, \$10M Stolen, juin 2018
- BleepingComputer – Malware Attack Disables ATMs in Chile, 2018
- Comparitech – Cyber Attacks in Latin America, 2022