Club de la sécurité de l'information français

Panorama de la cybercriminalité année 2016

Paris, 11 janvier 2017

Evénement organisé avec le soutien de nos sponsors

Club de la sécurité de l'information français

Les Banques : une cible de choix en 2016 avec des attaques de plus en plus diversifiées

Gérôme BILLOIS
Wavestone

@gbillois

L'environnement du SI bancaire

Systèmes clients


TPE


DAB


Professionnels

Systèmes exposés


Banque en ligne

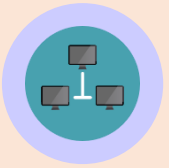

Flux interbancaires
(SWIFT, EDI, SEPA…)


Grand Public


Tiers
(Partenaires, startup…)

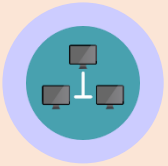
Interne


Monétique


SI Support

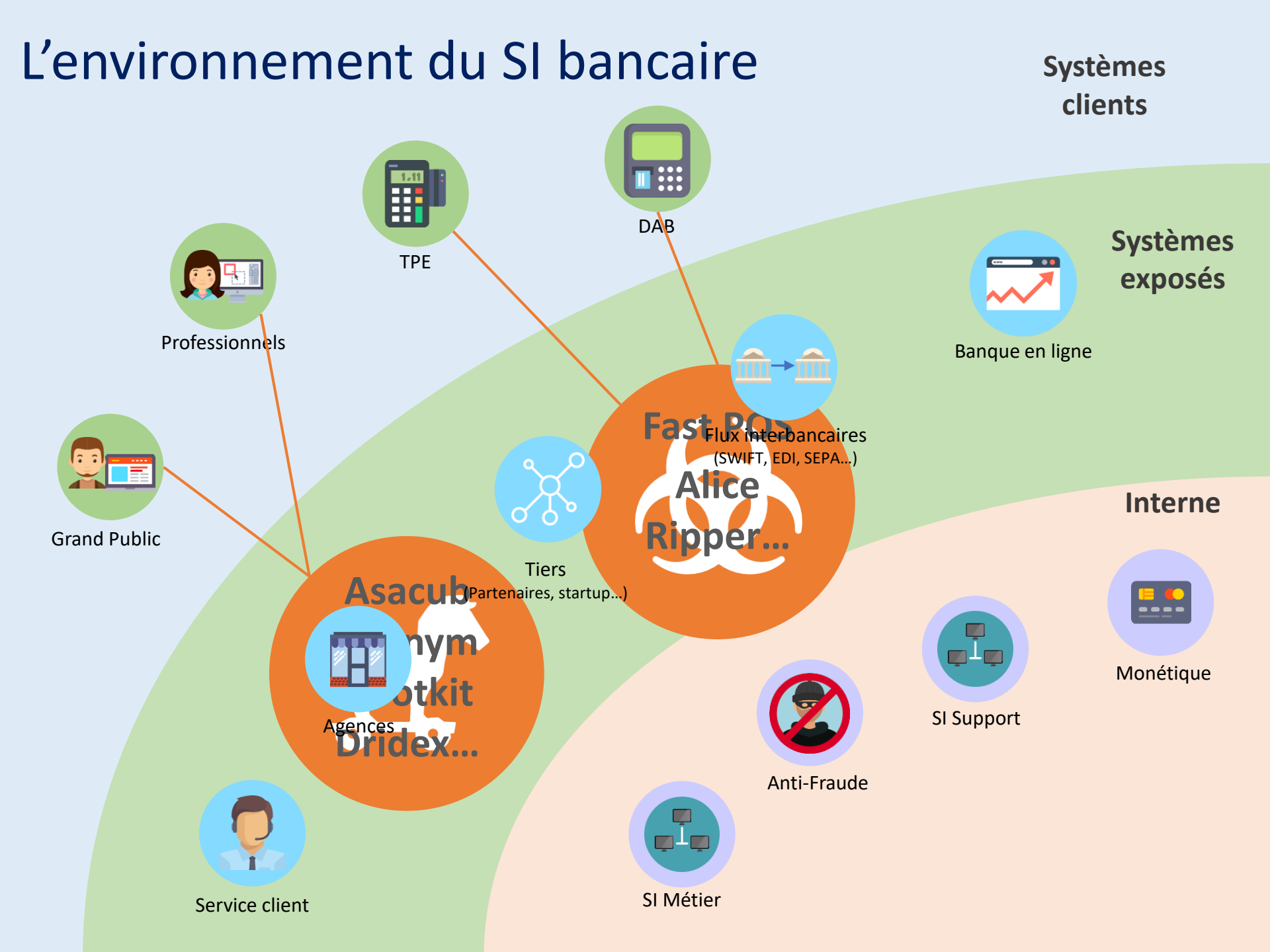

Anti-Fraude


Agences

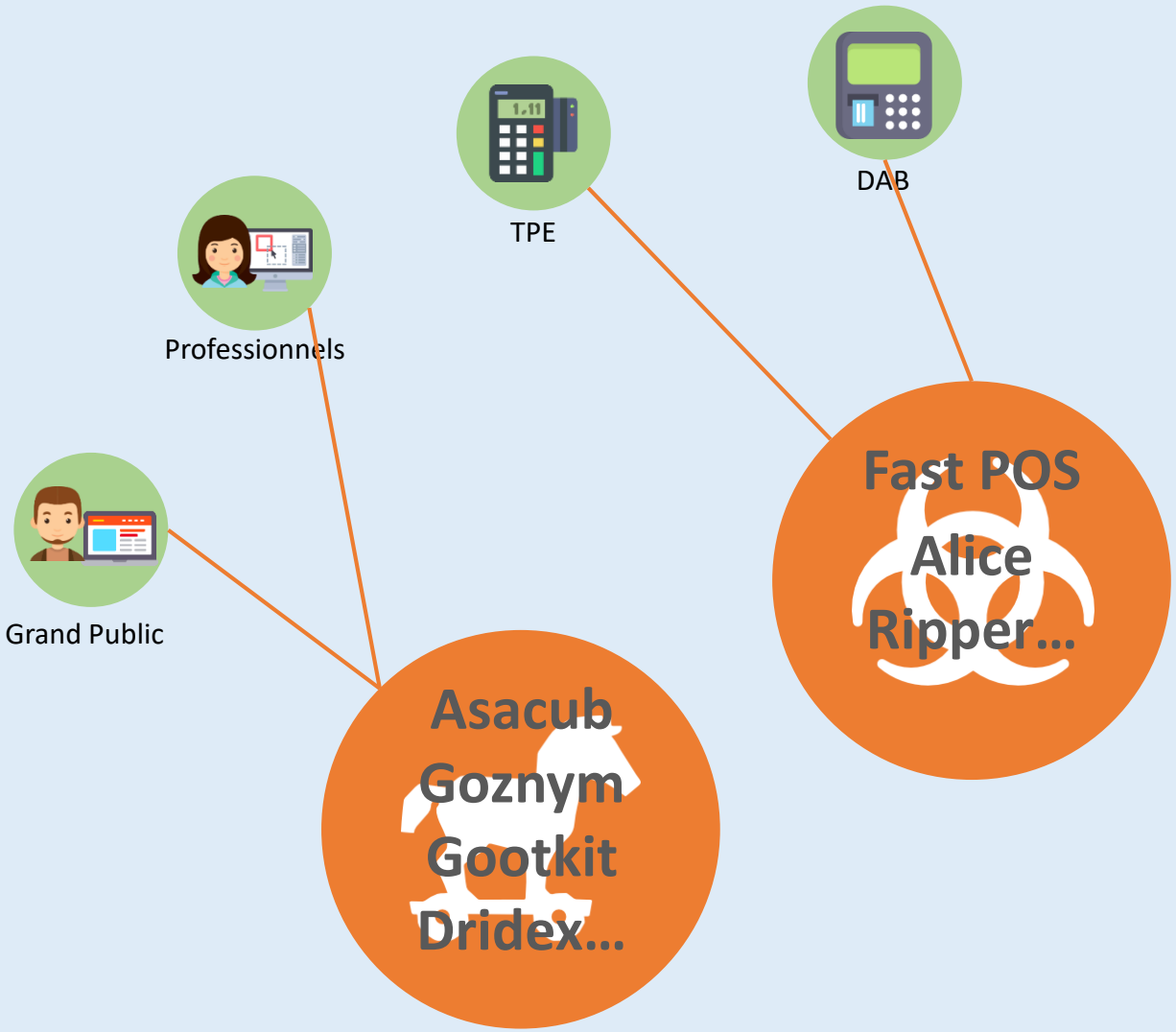

SI Métier


Service client

L’environnement du SI bancaire



Des attaques fréquentes en 2016



Des attaques fréquentes en 2016

Systèmes clients

DAB

TPE

Professionnels

Grand Public

Les **Skimmers:** du plus visible…

Des attaques fréquentes en 2016

Systèmes clients

TPE

DAB

Professionnels

Grand Public

Les **Skimmers:** du plus visible…

Des attaques fréquentes en 2016

Systèmes clients

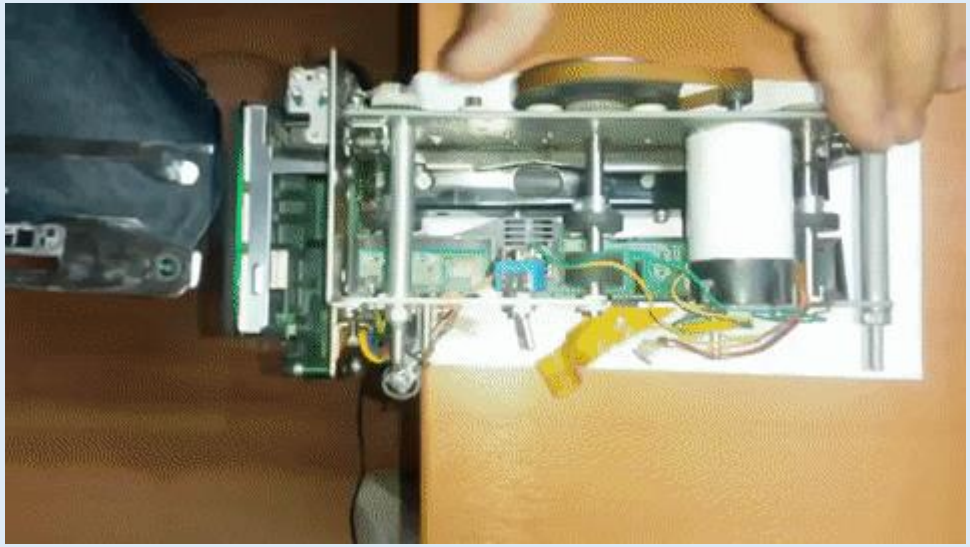
DAB

TPE

Professionnels

Grand Public

Au plus discret : Insert Skimmer



Des attaques fréquentes en 2016

£2,5M dérobés à 9000 clients de la **Tesco Bank UK de manière massive**

Systèmes exposés

Banque en ligne

Flux interbancaires
(SWIFT, EDI, SEPA…)

Attaque **DDoS** par exemple contre **5 banques Russes ou contre HSBC**

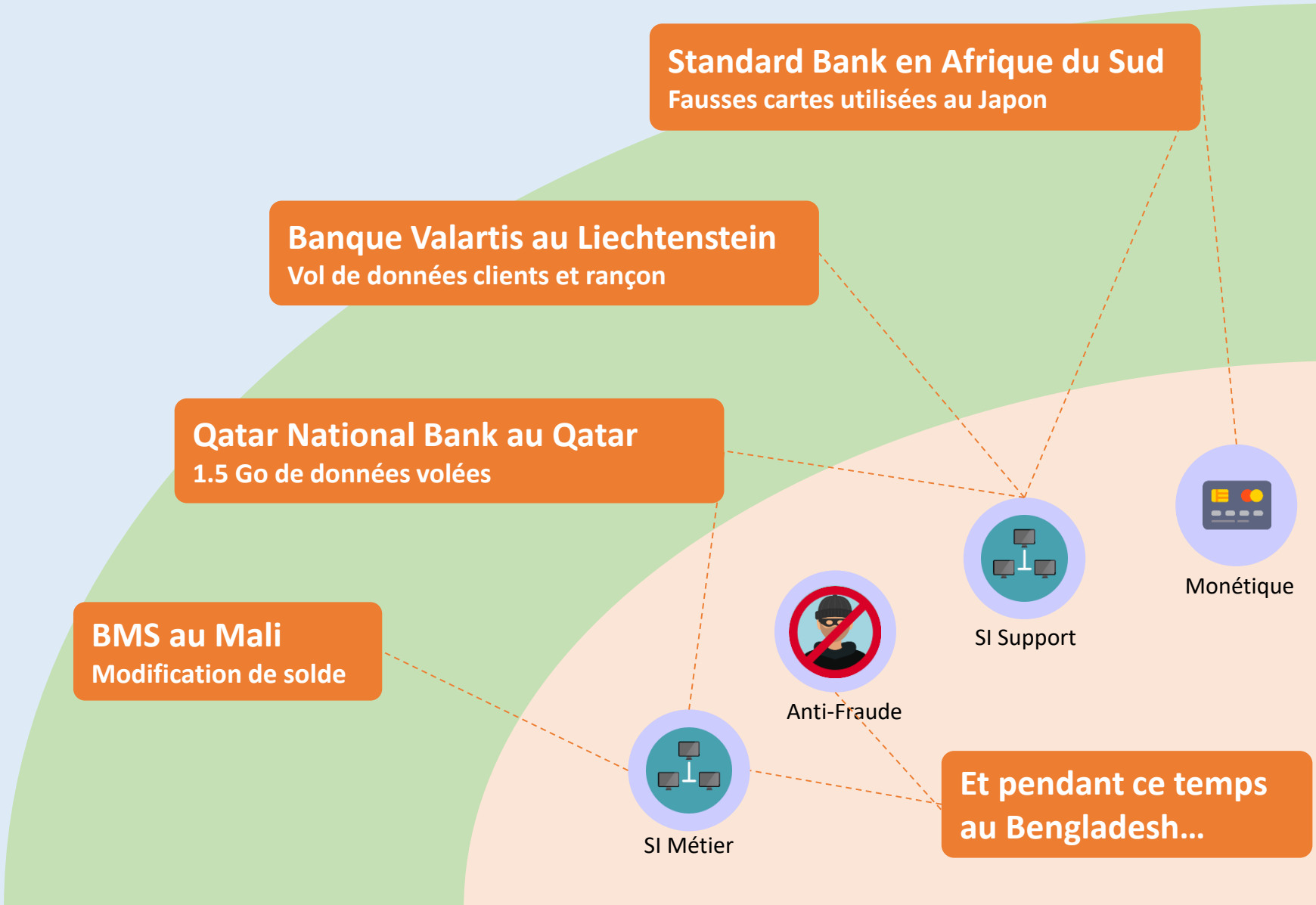
Tiers
(Partenaires, startup…)

Agences

Service client

Vol de $31M à la banques centrale Russe, vraisemblablement grâce à des identifiants clients contrefaits

Des attaques fréquentes en 2016



Cas Bank of Bengladesh : la route de la fraude

Au Bangladesh

4 Février 2016
Compte de la banque
à la FED
35 transactions $951M

La New York Fed
bloque 30 transactions
pour $850M à cause
d'un manque de détails

La New York Fed
valide
5 transactions
$101M

PanAsia Banking&Deutsche Bank
bloque 1 transactions
pour $20M à cause d'une typo

Les fonds arrivent
aux Philippines

La Rizal Commercial
Bank valide
4 transactions
$81M

Les fonds
sont
blanchis

Weikang Xu
$31M

Solaire casino
$29M

Eastern Hawaï Leisure
$21M

Cas Bank of Bengladesh : une attaque préméditée

Préparation → **1 Attaque** → **2 Détection** → **3 Résultat**

Mai 2015

- Ouverture de comptes bancaires sous de fausses identités
- Création des outils de la cyber attaque
- Première intrusion et identification des serveurs SWIFT

Du 4 au 6 Février 2016

- Emission des ordres de transaction
- Déploiement du Malware sur les postes de travail utilisés pour les virements SWIFT
- Actions sur les systèmes anti-fraude pour effacer les traces des opérations

Du 5 au 8 Février

- Première alertes levées a cause d'incidents pour l'impression de transactions
- Découverte de la fraude et tentative de recouvrement des fonds

81 millions de dollars volés

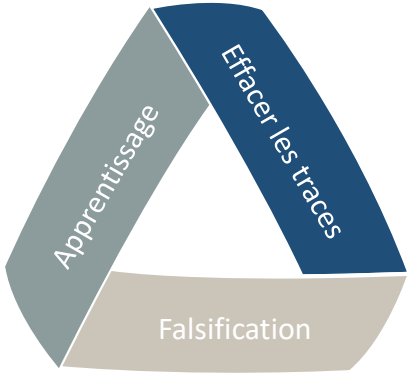
Démission du CEO de la Bank of Bangladesh

Cas Bank of Bengladesh : l'intrusion

1. Intrusion dans le système d'information de la Bank of Bangladesh
2. Vol des identifiants des responsables des opérations SWIFT, permettant de créer, approuver et exécuter des transactions via la FED à New York
3. Emission de 35 transactions frauduleuses
4. Suppression immédiate de toute trace générée par les hackers à l'aide d'un malware spécifiquement développé

Le malware utilisé

Observe quotidiennement les transactions légitimes



Efface les enregistrements des transactions frauduleuses dans la base de données locale

Intercepte les **confirmations de transactions** et modifie leur contenu avant impression

Cas Bank of Bengladesh : Les conséquences

12 May 2016

A new bank targeted in Vietnam

Malicious PDF reader

Modification of the display of transaction confirmation files

January 2015

Ecuador Bank victim since last year

US$12M stolen,

2,8 recovered. Wells Fargo sued for negligence

13 June 2016

Hedge fund targeted by the attackers

First similar attacks detected against companies specialized in asset management

Last updated: May 13, 2016 6:01 pm

Vietnamese bank hit by cyber heist

Martin Arnold in London

THE WALL STREET JOURNAL.

Subscribe Now | Sign In

SPECIAL OFFER: JOIN NOW

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life Real Estate

MARKETS | FINANCIAL REGULATION

Now It's Three: Ecuador Bank Hacked via Swift

Cybercriminals stole $9 million in 2015 from an Ecuador bank in attack similar to one against Bangladesh's central bank about a year later

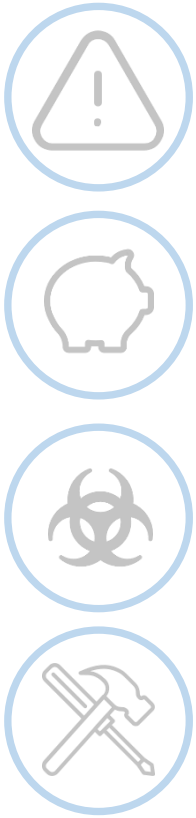
Infrastructure

Hackers targeting SWIFT banks also targeted US moneymen: Hedge funds at risk

Threat detection outfit hands research results to Feds

En réaction, SWIFT lance un programme mondial pour contrer ces nouvelles menaces

Quelles conclusions en tirer ?



Oui, les clients et les systèmes exposés sont (et seront) toujours attaqués

Mais il y a une tendance à des attaques plus en profondeur

Y compris sur les systèmes anti-fraude

Besoin d'une approche globale de la cyber sécurité

Sources

https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/

http://www.hackmageddon.com/2016/08/30/1-15-august-2016-cyber-attacks-timeline/

https://www.fireeye.com/blog/threat-research/2016/08/ripper_atm_malwarea.html

https://securelist.fr/blog/recherche/64562/trojan-asacub-le-spyware-devenu-malware-bancaire/

https://www.fireeye.com/blog/threat-research/2016/10/operations_of_a_braz1.html

http://krebsonsecurity.com/2016/07/kimpton-hotels-probes-card-breach-claims/

http://blog.trendmicro.com/trendlabs-security-intelligence/fastpos-quick-and-easy-credit-card-theft/

http://www.ewdn.com/2016/12/07/russian-banks-targeted-by-massive-cyberattacks/

https://www.scmagazine.com/big-malware-moments-of-2016-part-1/article/571100/

http://money.cnn.com/2016/12/02/technology/russia-central-bank-hack/

https://www.ft.com/content/7faf84c4-0c98-11e6-b41f-0beb7e589515

http://www.fbf.fr/fr/files/ABKG54/Rapport-2015-OSC-05072016.pdf

https://www.grahamcluley.com/atm-malware-cobalt-hacking-gang/

http://fortune.com/2016/11/21/hackers-atms/

http://thehackernews.com/2016/03/credit-card-skimming-hack.html

http://thehackernews.com/2016/05/japan-atm-hack.html

http://linkis.com/maliactu.net/GAPGd