Processus de réponse aux incidents

Desjardins

Coopérer pour créer l'avenir

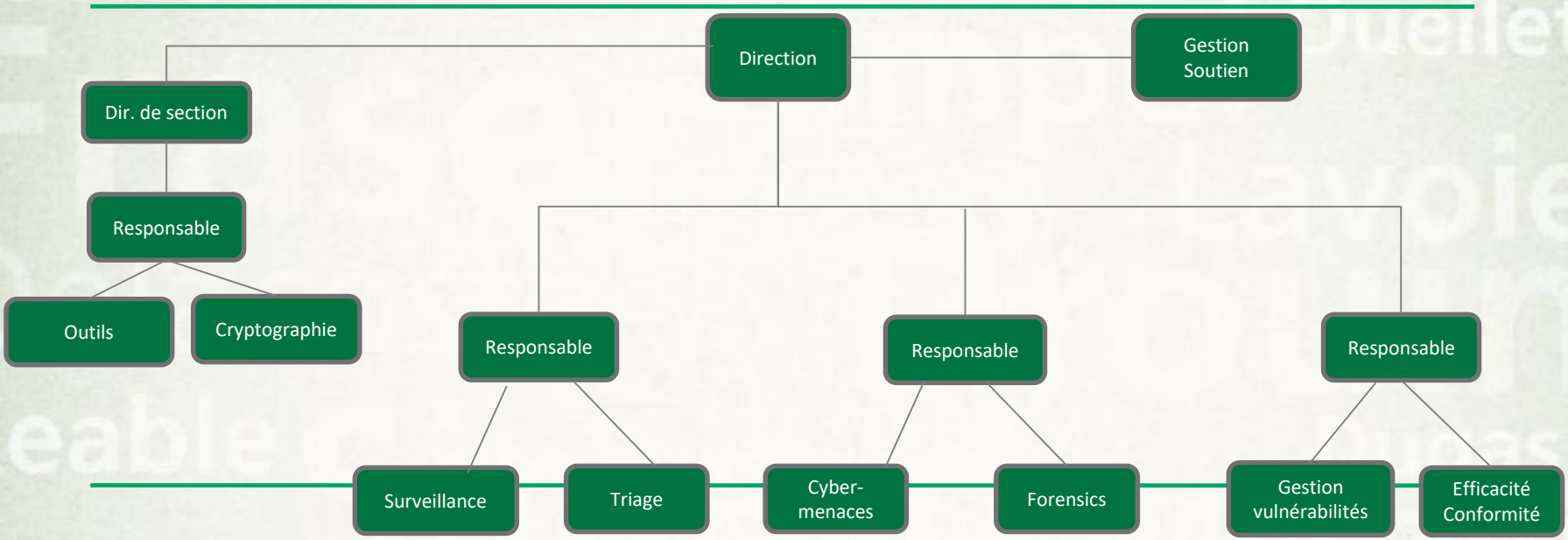
Contenu

- Le CSS
  - Présentation
  - Organigramme/Domaines d’expertise
  - Cas vécus
  - Communications
  - Questions

Le Centre de surveillance de la sécurité (CSS)

- Le CSS fait partie de la Direction Surveillance et Sécurité de la Direction principale Sécurité et Télécommunications.
- Le CSS (ou SOC-Security Operation Center) assure la surveillance de l'ensemble des infrastructures technologiques de Desjardins.
  - Le CSS est une équipe d'exploitants chargée de faciliter la mise en place de la sécurité TI de Desjardins par la surveillance des environnements et la détection de cyber menaces
- Près de 50 ressources sur 2 sites (Lévis et Montréal)

Organigramme du CSS



Desjardins

Coopérer pour créer l'avenir

Domaines d’expertise CSS
Gestion des cyber menaces

- Service de renseignements sur les cyber menaces
  - Analyse des renseignements provenant de l’internet, de nos partenaires internes et externes
  - Gestion des améliorations de nos cas de surveillance
  - Analyse forensics - Contrevenants technologiques

Domaines d’expertise CSS
Gestion des événements de sécurité

- Prise en charge initiale des événements de sécurité
- Gestion des requêtes opérationnelles de service

Domaines d’expertise CSS
Gestion des vulnérabilités

- Prise en charge de la gestion des vulnérabilités et suivi des mesures correctives
  - Analyse des balayages de vulnérabilités
  - Production de rapports sommaires et détaillés des vulnérabilités et des principales mesures correctrices à appliquer

Domaines d’expertise CSS
Gestion des infrastructures de sécurité/Cryptographie

- Gestion de l’ensemble des outils de surveillance et de détection des événements de sécurité
- Gestion de l’ensemble des certificats numériques du Mouvement

Cas vécus

- Fuite de données externes
- SWIFT - Society for Worldwide Interbank Financial Telecommunication
- DynDNS - Lenteurs Internet généralisées - Attaque Déni de services

Fuite de données externes

MasterCard

American Express

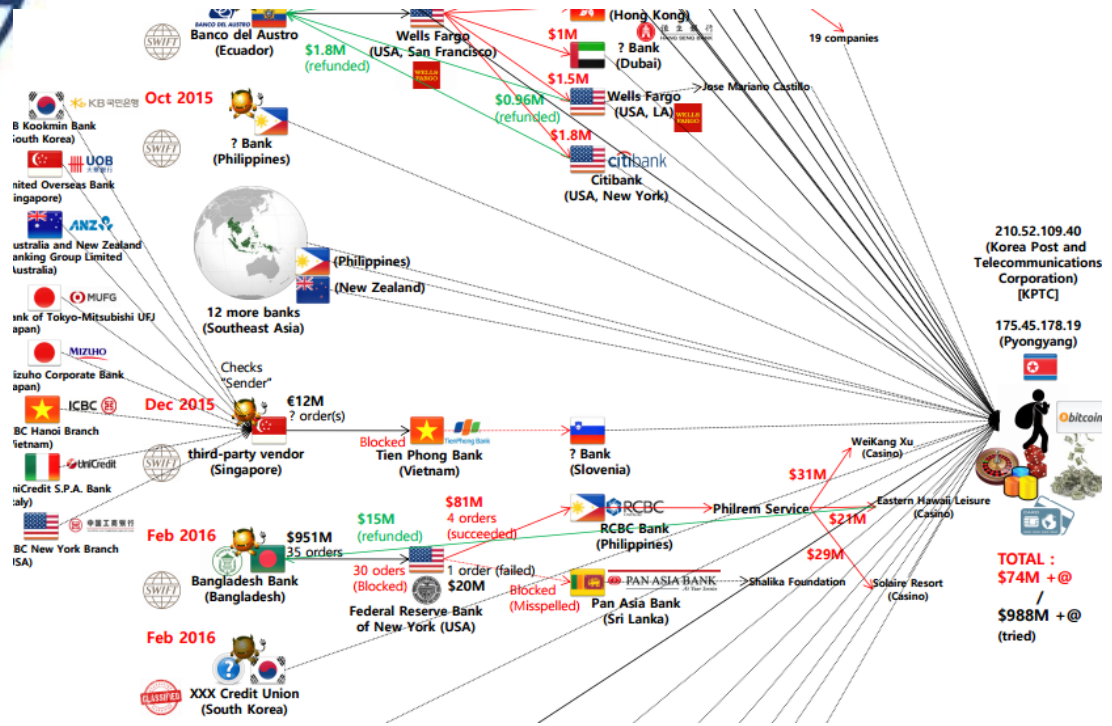
PayPal

Diners Club

Desjardins

Coopérer pour créer l'avenir

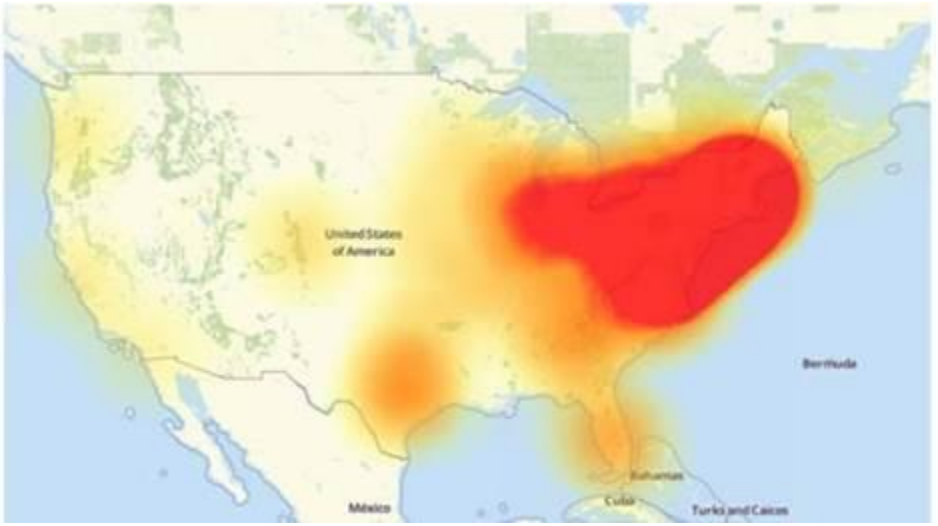
SWIFT - Society for Worldwide Interbank Financial Telecommunication



Desjardins
Coopérer pour créer l'avenir

DynDNS - Lenteurs Internet généralisées - Attaque Déni de services

DynDNS



Desjardins
Coopérer pour créer l'avenir

Communications

Desjardins

CTI - CYBER THREAT **INTELLIGENCE**
Direction Surveillance et Sécurité opérationnelle, Technologies

Avis CSS - Lenteurs Internet généralisées - Attaque Déni de services Dyn DNS
21 octobre 2016

Bonjour,

Plusieurs grands noms d'internet dont Twitter, Spotify ou eBay ont été gravement perturbés vendredi aux États-Unis par une attaque informatique dirigée contre le prestataire de services Dyn DNS. D'autres sites comme Ici.radio-canada.ca semblent aussi affectés. L'attaque dite par déni de service (DDOS) a commencé débuté vers 7h11 (heure du Québec) et a visé la société Dyn, qui redir internet vers les hébergeurs et traduit en quelque sorte des noms de sites en adresse IP.

Elle n'est pas sans rappeler les attaques DDOS contre OVH et Krebs mentionnées dans le [Desjardins Cyber hebdo] du18-24 SEPTEMBRE 2016 et les attaques de « Internet of things » relié à Mirai mentionnées dans le [Desjardins Cyber hebdo] du - 0 OCTOBRE 2016
Ces ralentissements ne sont pas p

Portait Desjardins

- Le CSS a validé cette infor
- Le CSS a validé cette infor

Actualité de la dernière semaine
04 au 10 décembre 2016

RANSOMWARE Un regain de *ransomware* cette semaine pour quelques utilisateurs qui ont vu leurs fichiers être encryptés après avoir ouvert un fichier attaché malveillant. Il s'agissait d'un courriel qui, en apparence, semblait venir d'un *scanner* à l'interne. Nous avons tout de même limité les dégâts en supprimant le courriel pour une quarantaine d'utilisateurs qui n'avaient pas encore ouvert le fichier.

SHA-1 Le décompte est commencé. Les échéanciers de la part d'Apple, Microsoft, Google et Mozilla sont connus en ce qui a trait au moment où leurs navigateurs cesseront de faire confiance aux sites web qui utilisent encore des certificats SSL SHA-1.

Google Chrome: À la fin de janvier 2017 avec la sortie de la version 56, Chrome cessera de reconnaître tous les certificats SHA-1 SSL et affichera un message d'avertissement.

Mozilla Firefox: Dès janvier prochain avec la version 51 de Firefox, le navigateur affichera une connexion non sécurisée pour tous les sites qui utilisent SHA-1.

Desjardins
Coopérer pour créer l'avenir

Questions