Chambre Monégasque des
Nouvelles Technologies

Guide des bonnes pratiques :

Comment se prémunir des fraudes téléphoniques (phreaking) ?

CHAMBRE MONEGASQUE DES NOUVELLES TECHNOLOGIES
Le Coronado - 20, avenue de Fontvieille - MC 98000 MONACO
Tél. : +377 92 05 38 92 - Fax : +377 92 05 20 04 - www.chambre-nt.mc - contact@chambre-nt.mc

Chambre Monégasque des
Nouvelles Technologies

1- Les fraudes

Elles se font en créant artificiellement du trafic téléphonique vers des numéros surtaxés, à coûts partagés, ou dont le numéro appelé est plus cher que la moyenne.

Elles ont pour objet de générer une explosion des factures téléphoniques au profit de réseaux mafieux ou de « simples » malfaiteurs.

Les pirates sont techniquement compétents et très organisés. Ils s'introduisent dans les systèmes au travers des connexions internet ou des lignes téléphoniques. Ils semblent venir majoritairement d'Europe de l'Est et d'Asie mais, à ce jour, personne n'a encore réussi à les localiser. Le problème réside principalement dans le fait que les différentes Polices Nationales doivent intervenir hors de leurs propres frontières, et donc hors de leurs propres prérogatives nationales.

Une des actions des pirates consiste à utiliser frauduleusement les installations téléphoniques des entreprises afin de générer du trafic téléphonique international illicite (cf. : paragraphe 2)

Les actions frauduleuses peuvent être également générées à partir de cartes SIM volées.

Elles se font principalement en dehors des heures ouvrées pour réduire les possibilités de détection.

2- Comment les pirates Télécoms s'enrichissent-ils ?

Il existe plus de 5000 opérateurs Télécoms dans le monde. Les opérateurs Télécoms achètent et revendent à leurs clients des appels téléphoniques vers toutes les destinations nationales et internationales. Les opérateurs font transiter des milliards de minutes de communication chaque année. Les opérateurs achètent selon des tables de routages particulièrement pointues, permettant de faire transiter les appels de leurs clients au meilleur coût.

Il existe des centaines de sociétés spécialisées dans la revente de tarifs Télécoms. Ces sociétés sont surnommées des Carriers. Les plus importants Carriers exploitent des liaisons dédiées entre les pays, telles que les liaisons transatlantiques. D'autres plus petits se contentent de faire du troc de minutes. Ceux-ci sont les fournisseurs privilégiés des pirates Télécoms.

Les pirates génèrent du trafic téléphonique à partir des installations de plusieurs centaines d'entreprises pour revendre ce trafic Télécom à des Carriers. Les Carriers revendent les minutes de communication, ainsi qu'aux opérateurs qui les revendent à leurs clients.

Les numéros surtaxés/serveurs payants (sites « roses » par exemple) sont également une manne pour les fraudeurs qui, soit les possèdent, soit proposent à leurs propriétaires de maximiser (contre rémunération) l'utilisation de leurs numéros/serveurs.

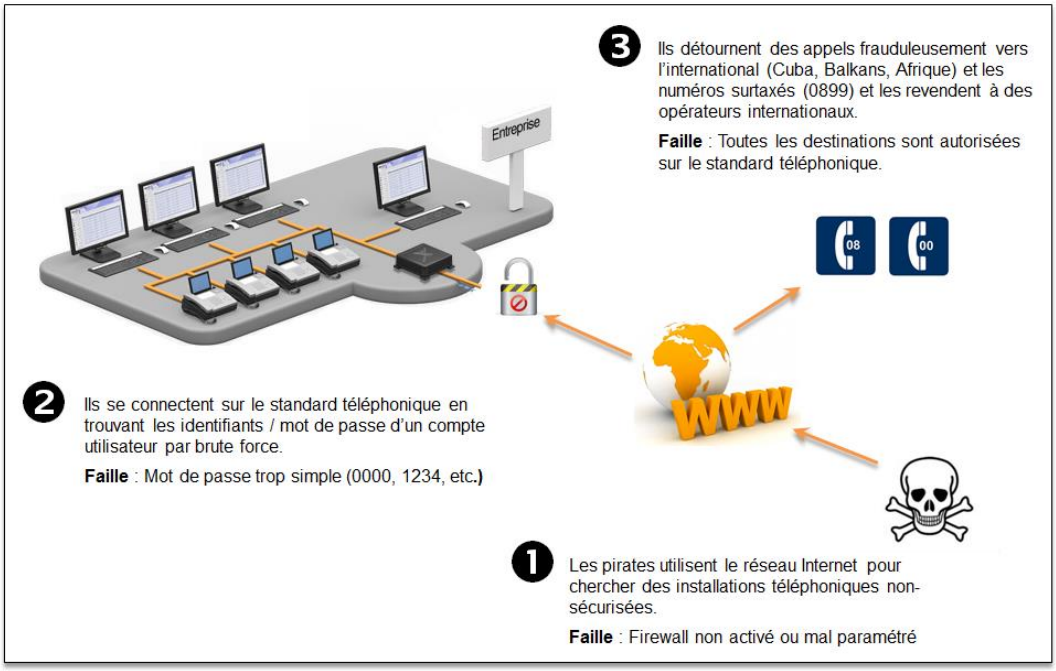
Chambre Monégasque des
Nouvelles Technologies

3- Les principales attaques

Nous connaissons à ce jour deux méthodes utilisées par les pirates Télécoms :

a. Le piratage via le réseau Internet

La nouvelle génération de standard téléphonique (Téléphonie IP) est totalement intégrée au réseau informatique de l'entreprise qui lui même est relié à Internet. Cependant, un pare-feu informatique (Firewall) mal configuré, ne protègera pas efficacement le standard téléphonique. Les pirates peuvent alors s'introduire dans le système téléphonique de l'entreprise via une connexion Internet. Si le logiciel de gestion et d'administration n'est pas correctement protégé par un mot de passe, ils disposeront de toutes les facultés pour programmer des renvois d'appels vers des numéros internationaux surtaxés.



b. Le piratage via les connexions commutées

Les pirates s'introduisent dans le système téléphonique de l'entreprise via les lignes extérieures (Réseau Téléphonique Commuté numérique RNIS ou analogique).

Leur premier objectif est de détecter la présence sur le système téléphonique des boites de messageries vocales non sécurisées (mots de passe simplistes de type 1234, 0000…etc)

En utilisant des fonctions spécifiques du système téléphonique, ils renvoient ces boites vocales vers des numéros internationaux surtaxés.

Leur deuxième objectif est de se connecter au logiciel de gestion et d'administration du système en utilisant une fonction modem. Si le logiciel de gestion et d'administration n'est pas correctement protégé par un mot de passe, ils disposeront de toutes les facultés pour programmer des renvois d'appels vers des numéros internationaux surtaxés.

4- Protection mise en place par Monaco Telecom (le FMS)

a. Protection, alertes et analyses

Afin de protéger ses clients contre les usages malveillants, Monaco Telecom a mis en place un système d'analyse des anomalies dans les comportements d'appel, qui permet, avec un délai de quelques heures, d'identifier des appels anormaux par quantité et destination, et d'intervenir.

Le Fraud Management Service (FMS) est un système techniquement avancé et efficace. S'agissant d'un système curatif, il ne peut toutefois pas empêcher les usages malveillants, mais seulement en limiter la durée.

La matrice des alertes remontées par le FMS s'inscrit entre deux axes :

1. les destinations :
   - « Grise »: destinations très chères (numéros surtaxés étrangers, destinations très coûteuses, satellite, etc…)
   - « Rose »: destinations chères

2. les volumes de communication en fonction de 4 typologies de clients et/ou numéros appelés:
   - Abonné National
   - Abonné National VIC (*)
   - Numéros appelés répétitifs (Abonné National &International)
   - Carriers International

(*) VIC : Very Important Consumers in terms of volume

b. Les actions de Monaco Telecom suite à une remontée d'alerte

- Le Client est contacté en heures ouvrées pour vérifier si le trafic constaté est de son fait ou pas.
- Si l'alerte intervient en heures non-ouvrées et que le Client n'est pas joignable, les Techniciens de Monaco Telecom interviennent :
    - Pour les lignes fixes: mise en place d'une restriction de service qui peut s'établir à des niveaux (fixés) différents d'autorisation d'appels sortants (Monaco, France, Europe hors pays baltes, USA, Canada, etc…).
    - Pour le mobile: suspension de la ligne mobile.

Quel que soit le degré éventuel de sophistication de ses alertes, Monaco Telecom ne peut empêcher les fraudes filaires de se produire car le problème ne se trouve pas sur son réseau. Il se traite au niveau de la sécurité des installations téléphoniques des Abonnés, aussi bien des entreprises monégasques qu'étrangères (dans le cas de fraude acheminée par un autre Carrier). Il y a donc lieu d'appliquer des règles de bonne conduite.

5- Les règles de bonne conduite préconisées par les installateurs aux entreprises utilisatrices

a. Sur le filaire

- Votre **installateur** a un devoir de conseil et de mise en garde à votre égard. Il se fera un plaisir de définir avec vous une politique de sécurité adéquate, en particulier concernant la **définition des niveaux de service (restriction) par utilisateur**.

- Isolez physiquement et logiquement votre installation : **sécurisez et isolez votre serveur téléphonique** dans un espace dédié et dont l'accès est restreint (fermé et accessible seulement aux personnes habilitées) comme vous le feriez pour vos serveurs informatiques.

- Nommez une personne au sein de votre entreprise formée aux procédures de changement des mots de passe.

Chambre Monégasque des Nouvelles Technologies

Il est impératif de mettre en place au sein de l'entreprise **une politique de gestion des mots de passe**. Il faut les personnaliser **dès l'installation, et les modifier régulièrement.** Les mots de passe doivent être complexes, notamment ceux des comptes administrateurs.

- **Ne jamais conserver les Comptes d'Administrateurs par défaut,** et établir, lorsque c'est possible, une hiérarchisation des profils des comptes d'administration.
    - Par exemple :
        - boîte vocale simple avec enregistreur ou assistance personnelle ;
        - choisissez le renvoi d'appel vers l'extérieur uniquement si cela est nécessaire pour l'utilisateur ;
        - si votre activité ne nécessite pas d'appeler à l'étranger, optez plutôt pour un accès national. Ceci peut s'appliquer également aux numéros surtaxés.

- Les constructeurs de systèmes téléphoniques mettent régulièrement à jour le logiciel pour améliorer la sécurisation de leurs produits**, choisissez un niveau de contrat qui intègre ces évolutions.**

- **Vos partenaires (Constructeur, Intégrateur ou Installateur, Opérateur) sont régulièrement amenés à vous informer** ou vous alerter sur la sécurité de vos systèmes, restez vigilant quant à ces communications (courriers, mails…). N'hésitez pas aussi à leur poser vos questions.

b. Sur le mobile, le roaming reste un risque

- Signaler immédiatement le vol de votre mobile à votre opérateur pour la suspension de la ligne.
- Déposer plainte auprès de la Sureté Publique en fournissant votre n° d'IMEI (figurant sur la boîte d'emballage et la facture d'achat du téléphone) pour que votre opérateur puisse rendre inutilisable votre mobile. (Projet de loi 934, article projeté 389-11-6, article L34-3 du code des postes et des communications électroniques).