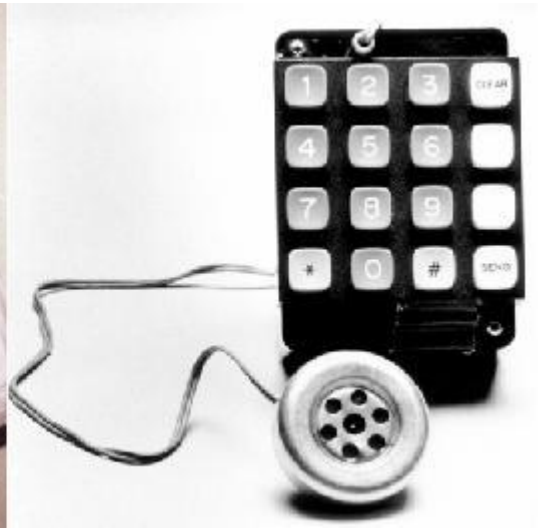
PHREAKING



Pascal ENZINGER
Commissaire en Chef

Service Nouvelles Technologies du SPJ

24, rue de Bitbourg
Luxembourg - Hamm

PHREAKING

Étymologie et Origine:

Le mot anglais **phreaking** est obtenu par la contraction de **phone**, pour téléphone, et **freak**, signifiant un marginal, ou personne appartenant à une contre-culture.

Le phreaking est né aux États-Unis dans les années 1970.

Un des mythes fondateurs du phreaking est l'histoire de Captain Crunch qui avait utilisé un sifflet trouvé dans une boîte de céréales pour accéder à des fonctions spéciales du central téléphonique.

En effet, le son émis par ce sifflet avait la même fréquence que le signal utilisé pour piloter le central téléphonique.

P H R E A K I N G

Aujourd'hui:

- Vaste répartition de centrales téléphoniques (PABX) suite au progrès technique
- Peuvent être trouvées dans toute entreprise même dans les domiciles privés. (FritzBox Router)

  - Manipulation de la centrale pour faire transiter des appels

But:

➢ Appeler des numéros de plus value
(pex. +23221204253 Sierra Leone)

➢ Services Call by Call
(faire des appels par un autre operateur à un meilleur prix)

PHREAKING

Numéros de Plus Value:

Maxtis Telecom **République Tchèque**

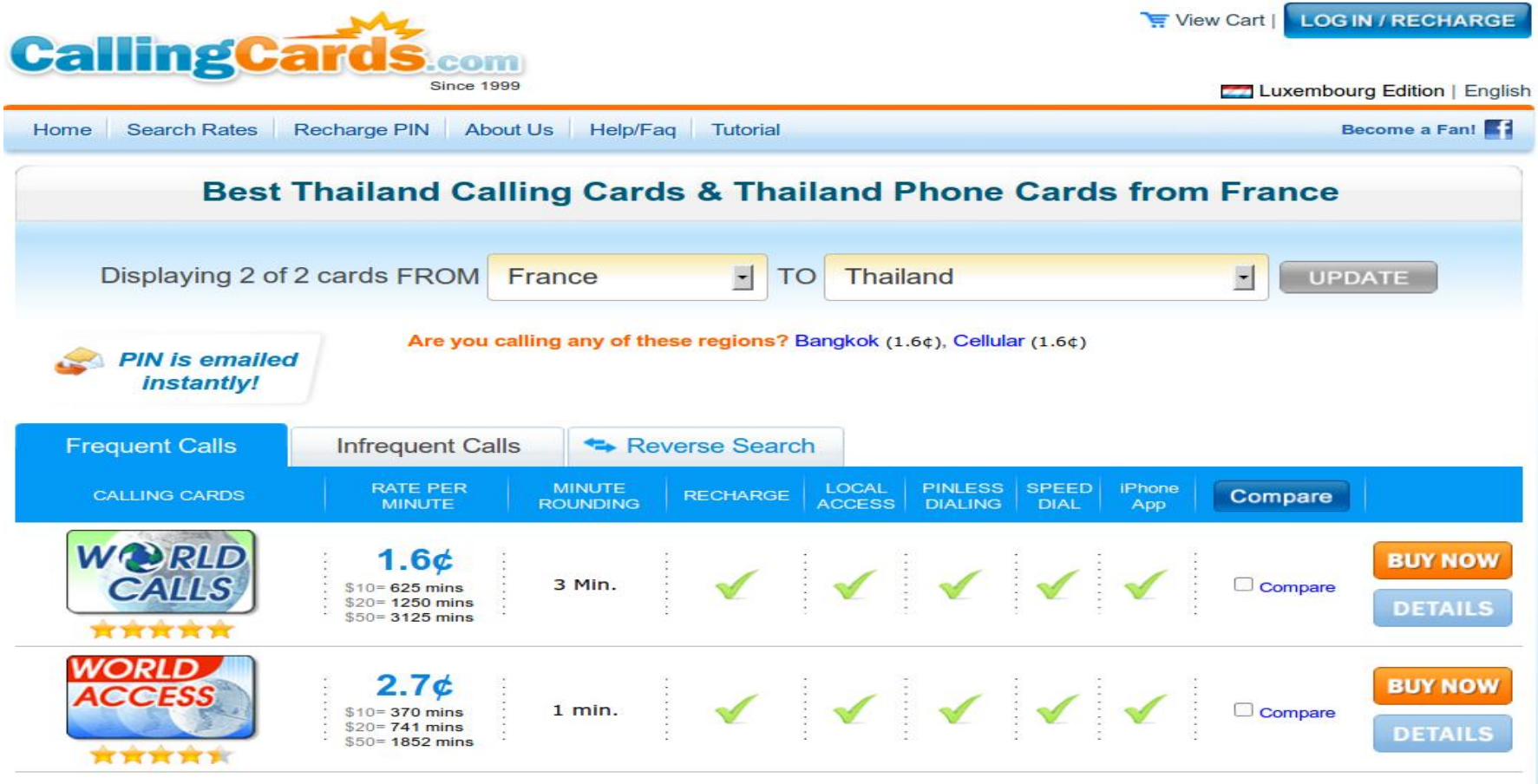
www.maxtis.com

PHREAKING

Services Call by Call:

www.callingcards.com

Calling Cards



P H R E A K I N G

Quelques chiffres:

- 16 Plaintes traitées par le SPJ NT depuis mi 2010

Préjudice:

- Entre 5.000 € et 200.000 €
- Dans la majorité des cas entre 15.000 € et 30.000 €
  (P.ex.: Plainte d'une firme en 2011 qui a perdu 17.000 € en deux jours par des appels au Sierra Leone)

OUT	20121212	191301	23221203200	00:02:00	Sier.Leone
OUT	20121212	191507	23221203263	00:23:10	Sier.Leone
OUT	20121212	191510	23221203263	00:16:13	Sier.Leone
OUT	20121212	192651	23221203263	00:15:12	Sier.Leone
OUT	20121212	192844	23221203263	00:38:19	Sier.Leone
OUT	20121212	193957	23221203263	00:25:08	Sier.Leone
OUT	20121212	194944	23221203263	00:08:11	Sier.Leone
OUT	20121212	194948	23221203263	00:04:11	Sier.Leone

P H R E A K I N G

Cibles:

Tous types et marques de centrales téléphoniques sont concernés:

- Classique (Analogique / ISDN)
- VoIP (Voice over IP)
- Logiciels PABX Open Source (Asterisk, Freeswitch …)

Mais également, et à ne pas oublier !

- Sytèmes de Vidéoconférence, reliés à la centrale et / ou à l'Internet

Les spécifications et manuels des différents centrales téléphoniques peuvent être trouvés sur Internet.

P H R E A K I N G

Méthodes d'intrusion:

- Abus de l'accès pour la maintenance à distance
- Mots de passe standard inchangés (marqués dans les manuels du fabricateur)
- Mots de passe trop simples (numéro du poste = mot de passe)
- Failles connues et spécifiques pour certaines centrales, comme 'Dial per Zero'
- Voice Mailbox installée pour chaque poste
- Hacking du Routeur et / ou de la centrale sur des systèmes Asterisk / VoIP

➢ Dans la majorité des cas ces actions ont eu lieu pendant les weekends, jours fériés et les heures de fermeture.

P H R E A K I N G

Méthodes d'intrusion:

HACKING

WWW.FZ1.FR.FM

Hacking

Tous les documents que vous pouvez trouver ici sont à titre informatifs. Par leur lecture vous vous rendrez compte du manque de protections et de l'insécurité qui règne sur le réseau ainsi qu'au sein de la plupart des serveurs.

HACKONS LES PABX

1: C'est quoi un PABX ?

Un PABX (Private Automatic Branch eXchanger) est en fait un central telephonique qui gere les appels entrants est sortants. Il gere le reseau interne aussi bien que le reseau externe. Pour vous donner un exemple: Mr Lamer travail chez Grolame & Co. Monsieur Lamer veut telephoner... Pour cela, il decroche son telephone, il appuie sur `0' puis il compose son numero. Voila en gros a quoi un PABX peut servir.

Bon on y va alors. A quoi ca peut bien vous servir de savoir que Mr Lamer lamer peut phoner depuis son poste en faisant le 0' ??? D'abord vous devez comprendre a quoi ca ressemble un PABX.

o Chaque employe a un poste bien a lui, OK ?
o Chaque employe a une ligne directe (surement), OK ?
(surement car le PABX ne servirait a rien sinon, eh!).
o Tous les employes sont relie au PABX.

Bon voyons de plus pres comment ca marche maintenant: vous appelez le PABX.
Ensuite, une fois dans le PABX, vous pouvez etre redirige entre les differents postes ou services (les 4 derniers chiffres du numeront correspondent au numero du poste, par exemple 12 12 + numero de poste, comme 0003). 12 12 00 03 c'est bon, vous avez compris, et je vous vois dire que c'est facile une fois qu'on connait les 4 premiers chiffres. C'est les memes que ceux de l'entreprise. Ex: voici le numero de l'entreprise Grolame & Co, 12 12 00 05. Vous savez maintenant qu'il faut mettre 12 12 + pour avoir le numero de la ligne directe de l'employe (attention, les PABX en numeros verts ne fonctionnent pas pareil, vous n'avez pas de ligne direct dans ce cas la).

P H R E A K I N G

Suggestions contre mauvaises surprises:

- Soyez vigilants si vous avez du mal à avoir une ligne extérieure
- **TOUJOURS !** Changez **TOUS** les mots de passe / pin standard
  - Mercedes = mauvais choix !
- Mise à jour du firmware / logiciel, paramètrage correct
- Bloquer les préfixes internationaux trop exotiques (Afrique, Amérique du Sud)
- Voice Mailbox installée d'office pour chaque extension, besoin?
- Fonctionnalité DISA qui permet aux employés de faire transiter des appels internationaux de leur domicile par la centrale afin de téléphoner pour le tarif local, besoin ?
- Mettre en place un monitoring qui détecte des communications excessives. (Centrale téléphonique ou opérateur)

P H R E A K I N G

Où déposer plainte?

- En principe: votre unité de police la plus proche
- Centrales téléphoniques / Intrusion dans vos installations informatiques
  - Service de Police Judiciaire
  - Section Nouvelles Technologies

CIRCL
Computer Incident Response Center Luxembourg

Dans le cas d'intrusion dans un système informatique (serveur), contactez également le Computer Incident Response Center Luxembourg.

www.circl.lu

P H R E A K I N G

Où déposer plainte?

- D’abord, sécurisez votre système !
- Analyse du système afin d’établir le type d’attaque
- Rassemblez les preuves dont vous disposez
  - Données techniques (p.ex. fichiers Log, Courriels avec Header)
  - Listing Appels

- Dépot de plainte de préférence avec un technicien pour donner des explications nécessaires
- Assistance de votre conseiller personnel possible

P H R E A K I N G

QUESTIONS ?

Pascal.Enzinger@police.etat.lu