CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

CLUSIF

PABX IP et Sécurité

Solution de sécurité périmétrique

CheckPhone TECHNOLOGIES

CheckPhone TECHNOLOGIES

Le contexte


FRAUDE
ET
PERTES
FINANCIERES
IPBX
DENI DE
SERVICE
ECOUTES
INTRUSIONS DANS LE
SYSTEME
D'INFORMATION

Le hacking de PBX plus communément appelé fraude à la facturation représente un problème majeur pour le secteur des télécommunications et les entreprises

Le scénario

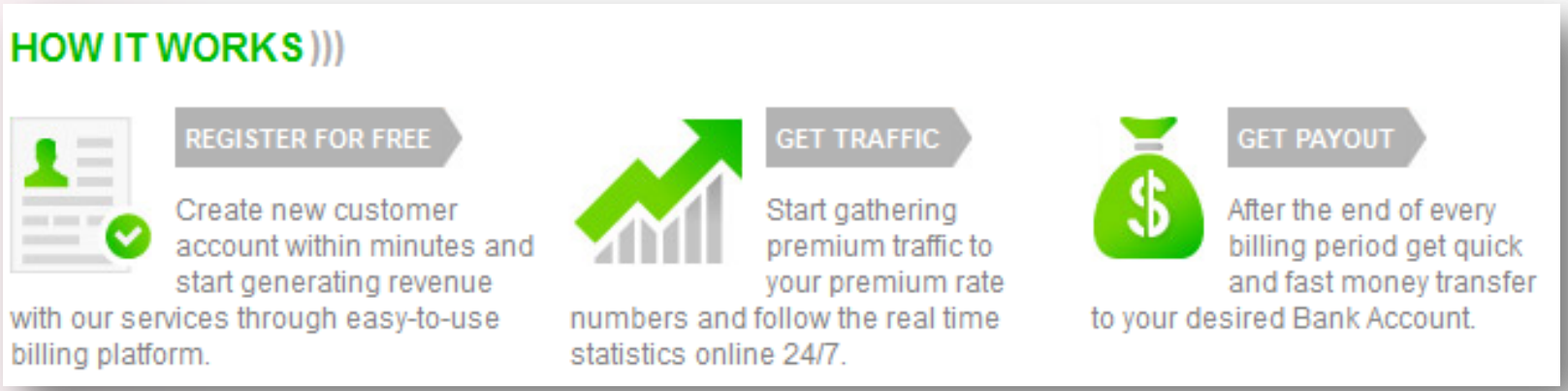
- Le monde ouvert des Communications Unifiées et des applications mobiles facilite de plus en plus l'accès au PBX
- Les fonctions natives disponibles dans un PBX facilitent la tâche du criminel qui souhaite hacker un PBX
- Le 1er symptôme du hacking de PBX se manifeste généralement lorsque l'opérateur de télécommunications notifie son client d'une explosion du nombre d'appels vers l'international
- A cette étape, la société en charge de la maintenance de la téléphonie bloque l'ensemble des communications sortantes

Pirater un PABX?

- Listes des mots de passe constructeurs
- Les entreprises à pirater
- Listes de vulnérabilités des systèmes
- Listes de numéros des messageries vocales

Compliqué?

- Les pirates louent des numéros payants à des sociétés spécialisées



La rémunération?

- Le paiement
  - Virements bancaires
  - Paypal
  - Western Union…
- Quelques conseils…
  - a) *Please try not to throw higher volumes than 3000 min / number / day per destination.*
    b) Make sure your traffic comes from diverse Cli's.
    c) Call durations should be kept under 20 min per call.
    d) not more than 3000 min per cli/day to all numbers on destination.
    HAVE A GOOD TRAFFIC!

Termination country	Range	Currency	Payout	Payment term
Argentina Buenos Aires	5411	EUR	0,15	30/45 EOM
Azerbaijan	9944001	USD	0,12	30/45 EOM
Azerbaijan Mobile	99440021	EUR	0,08	30/45 EOM
Azerbaijan Mobile	99440022	EUR	0,08	30/45 EOM
Belarus	375860	EUR	0,03	30/45 EOM
Bosnia	38765	USD	0,11	30/45 EOM
Dominica	17675	EUR	0,56	15/60 EOM
Emsat	88213	EUR	0,55	30/60 EOM
Emsat	88213	EUR	0,67	30/70 EOM
Estonia	372700	EUR	0,19	30/30 EOM
Estonia	372701	EUR	0,18	30/45 EOM
Estonia	372706	EUR	0,16	30/35 EOM
Estonia	372707	EUR	0,16	30/35 EOM
Estonia Mobile	372588	EUR	0,08	30/35 EOM
Estonia Mobile	372810	EUR	0,08	30/35 EOM
Estonia Mobile	372810	EUR	0,08	30/35 EOM
Globalstar	88180	EUR	0,47	30/60 EOM
Globalstar	88190	EUR	0,47	30/60 EOM
Grenada	14735077	EUR	0,2	30/60 EOM
Grenada	14735078	EUR	0,2	30/60 EOM
Grenada	14735079	EUR	0,2	30/60 EOM
Guinea	22455	USD	0,13	30/30 EOM
Guinea Mobile	22478	USD	0,13	30/30 EOM
Insat	88241	EUR	0,35	15/60 EOM
Italy Mobile	39319	EUR	0.05	30/70 EOM
Jordan	9626	USD	0,017	30/30 EOM
Kazakhstan	778800	EUR	0,12	30/35 EOM
Kazakhstan	780005	EUR	0,13	30/45 EOM
Kazakhstan	780905	EUR	0,13	30/45 EOM
Kazakhstan Premium	780905	EUR	0,14	30/45 EOM
Kosovo	377452	EUR	0,12	30/45 EOM

La méthode

- Les pirates louent des numéros payants à des sociétés spécialisées
  - Une entreprise de 200 personnes dispose d'un T2
  - L'attaquant pourra passer 15 appels simultanés
  - La fraude aura lieu du vendredi soir 19h au lundi matin 7h (60 heures)
  - Renvoi effectué vers un numéro payant en Espagne : 1,46€ l'appel + 0,13€ international

- Coût de la fraude pour l'entreprise victime :
  - 1,59€ par appel x 15 appels simultanés x 60 heures x 60 minutes =

  85 860€

- Gain pour le pirate :
  - 1.0173€ par appel x 15 appels simultanés x 60 heures x 60 minutes =

  54 934€

Drôle de jeux…et complexité

- L'impact financier d'un hacking de PBX déclenche généralement un drôle de jeux entre les différentes parties :
  - L'entreprise
  - L'opérateur télécom
  - Les juristes/avocats
  - Le VAR ou installateur
  - Les autorités

Les conséquences

- La vaste majorité des cas de fraude reportés génèrent :
  - Très peu de procès
  - De la frustration
  - Des pertes financières souvent élevées
  - Une rupture de confiance entre les différents acteurs

Quelques questions…

- Accès vers le réseau public? L'accès est-il réalisé au travers de trunks SIP?
- Possédez-vous un PBX IP ou un PBX hybride?
- Possédez-vous un système de voicemail IP?
- Sécurisez-vous votre infrastructure IP?
- Déployez-vous des Firewalls, des SBC?
- Quelle est la stratégie d'identification des téléphones et des utilisateurs?
- Est ce que votre stratégie de sécurité couvre la VoIP, les communications unifées? Quelle est cette priorité?
- Collectez-vous vos journaux d'appels?
- Comment sont analysées vos consommations, les montants de facturation inhabituels sont-ils gérés?
- Qui maintient et surveille vos politiques d'appels?
- Est-ce que les utilisateurs et les administrateurs sont informés des risques liés à la téléphonie?

Les contraintes

- Générations, versions
- Environnements hétérogènes
- Technologies (TDM, IP)
- Architectures distribuées
- Interopérabilité des systèmes
- Responsabilité d'exploitation
- Management des systèmes
- Centralisation de l'information
- Actions en temps réel

Une solution?

La définition d'une politique de sécurité inclut la téléphonie, et le déploiement d'une solution de sécurité périmétrique

Sécurité périmétrique

- Indépendance des I/PBX, des Opérateurs
- Facilités de maintenance
- Indépendance du média d'accès
- Gestion et Centralisation de l'information
- Visibilité, contrôle et management accrus
- Alertes et Interventions en temps réel

Conclusion

- La fraude fait supporter un coût énorme aux opérateurs et entreprises
- Le nombre d'acteurs (internes/externes) ainsi que le complexité des architectures nécessitent la définition d'une véritable politique de sécurité incluant la voix
- Protéger sa téléphonie et ses communications unifiées, au même titre que ses données, est indispensable

Merci!