12 mai 2014
Intrusion

Votre messagerie vocale peut-elle encore être facilement piratée ?

Des journalistes britanniques du site d'information "The Register" sont parvenus assez aisément à pirater la boîte vocale d'autres téléphones sans même en détenir le code PIN. Voici ce qu'il en est en France.

Avec Benjamin Bayart

Atlantico : Est-il encore possible de pirater un répondeur aujourd'hui, comme l'ont fait des journalistes britanniques (voire ici) ? Comment s'y prendre, concrètement ?

Benjamin Bayart : Tout dépend de ce qu'on entend par pirater. La majorité du temps, il suffit de taper la date de naissance de la personne que l'on souhaite "pirater" une fois qu'on est arrivé sur son répondeur. Dans 90 à 95% des cas, les gens utilisent ce code là pour sécuriser le répondeur, quand ils ne laissent pas le code classique. Accéder à ce niveau, qui permet d'écouter les messages, entre autres, est donc assez simple. Particulièrement aujourd'hui, où la date de naissance est une information des plus banales.

Pour autant, ça ne relève pas – à mon sens – du véritable piratage hostile. L'ordinateur qui contient le répondeur est un ordinateur comme un autre. Ce qui signifie qu'il a les mêmes vulnérabilités qu'un autre, et est sensibles comme un autre aux différentes failles. On peut donc, avec un peu d'agressivité, lui faire le même mal, mais tout de suite l'opération devient bien plus compliquée.

Du côté opérateur, cela l'est moins, dès lors qu'on parle de quelqu'un qui travaille dans la bonne équipe. La messagerie vocale est très voisine, techniquement, des boites mails. Un répondeur, c'est même une boite mail "déguisée" et qui contient des fichiers audios à la place de textes. Un ingénieur système qui a accès aux machines peut copier ces fichiers, voire demander à ce que tout fichier qui arrive sur une boite vocale soit également envoyé sur une autre, de la même façon qu'il peut le faire sur une boite mail. Ce qui peut être vraiment arrangeant quand on veut faire de l'écoute sauvage. Si on parlerait vraisemblablement de piratage dans la presse, j'ai tendance à y voir plus une forme d'abus de pouvoir de la part de ces gens qui disposent des droits, et les utilisent à des fins malhonnêtes.

Le vrai piratage, ça correspond à agresser un serveur pour prendre la main dessus. Et comme je le disais, le répondeur est un ordinateur comme un autre : il n'est pas plus sensible qu'un autre. Pour autant, quand on parle de serveurs, il est clair que les opérateurs réseaux auront tendance à faire attention que les banquiers, par exemples. A priori, il n'y a pas autant de choses critiques sur ces serveurs et c'est pourquoi les opérateurs sont vraisemblablement moins à cheval en termes de sécurité.

Qui, aujourd'hui, s'attaque aux boites vocales ? Peut-on parler de profil type ? Quels sont les motivations et les intérêts de ces gens-là ?

Un des exemples auquel on assisté remonte à 2011. Des journalistes anglais de News of the World avaient écouté la messagerie vocale d'une jeune fille de 13 ans portée disparue, et été accusés d'avoir piraté son téléphone. Cela a coûté très cher à l'organe de presse qui faisait ça, d'autant plus que certains indices ont été mis en péril à cause de cela.

Evidemment, on a également assisté à des tentatives pour accéder aux répondeurs de personnalités politiques, comme Kate Middleton par exemple. Finalement, écouter des messages peut servir à un peu tout, quand il s'agit d'en apprendre sur quelque chose ou quelqu'un. Les policiers, notamment, en font usage généralement, bien que cela m'apparaisse "légitime", puisqu'en France cet usage se limite aux enquêtes. Il n'est pas rare que la police ou les services secrets aient accès à des copies de la messagerie via l'opérateur.

Pour autant, c'est rarement sur un répondeur téléphonique que l'on trouve les informations sensibles. Quand quelqu'un communique un mot de passe, par exemple, il aura tendance à le faire par mail, ou alors de "vive voix" si c'est par téléphone. Mais il ne le laissera pas dans un message vocal. Si nous pouvons accumuler énormément d'informations, parfois très importantes, sur une boite mail, c'est nettement moins vrai sur un répondeur. Et pourtant, un mail n'est pas beaucoup plus sécurisé qu'une messagerie vocale, puisqu'il ne s'agit que de quelques manipulations pour en récupérer les identifiants. Le fait de prendre la main sur le mail de quelqu'un est extrêmement sensible en termes de sécurité.

C'est en général moins grave en téléphonie, puisque contrairement à la boite mail, nul parmi nous ne garde des centaines de messages. A mon sens, ceux qui s'adonnent à ce genre de piratages de boites vocales le font dans deux buts : soit il s'agit de surveiller quelqu'un, soit de se moquer de lui. Un conjoint trompé pourrait vouloir écouter les messages du partenaire infidèle, et j'ignore combien donneraient les journalistes de Closer pour accéder aux messages de Julie Gayet sur le répondeur du Président...

S'agit-il d'un processus facile à mettre en place ? Pourquoi ? Cela tient-il à la négligence des fabricants ?

Il suffit de connaître la date de naissance des gens en moyenne. Et ça est-ce que c'est une négligence des opérateurs ? Oui et non. La majorité des gens ne sont même pas au courant qu'il est possible d'interroger son répondeur depuis un autre poste. Il suffit d'appeler le numéro que l'on veut surveiller, de le laisser sonner dans le vide et de taper le code – la fameuse date de naissance – une fois qu'on arrive au répondeur.

Cela étant, écouter les messages de quelqu'un n'est pas invisible, bien que la majorité des gens n'y font pas attention. Le système de messagerie vocale présente différemment la situation selon que le fichier audio a déjà été écouté ou non. Ainsi un message qui n'a jamais été ouvert sera qualifié de "nouveau" tandis qu'un message déjà écouté écopera du qualificatif d' "ancien".

Ce sont les restes de l'époque des vieux répondeurs à cassettes. Il y a 20 ou 30 ans, il était de coutume de laisser un répondeur, branché sur la prise gigogne du téléphone quand on partait plusieurs jours, notamment en vacance. Et depuis l'endroit où l'on partait en congé, on appelait chez soi pour pouvoir écouter le répondeur en tapant le code. C'est strictement de la même façon que marche la messagerie d'un téléphone portable aujourd'hui. A ceci près qu'aujourd'hui, personne ne se sert de cette fonction, ou presque. C'est donc une faiblesse, une faille en termes de sécurité, qui n'apporte rien. A partir de là, on peut parler d'une certaine responsabilité des opérateurs, puisqu'il suffirait de désactiver cette fonction (tout en permettant à l'utilisateur de l'activer selon sa volonté) pour mettre un terme à ce problème. Sécuriser cette faiblesse serait enfantin.

Peut-on se protéger contre une attaque sur sa boite vocale ? Quelles sont les mesures à prendre ?

En premier lieu, changer le code de la boite vocale. Il faut savoir que les deux mots de passes les plus attendus par ceux susceptibles d'écouter vos messages sont les suivants : votre date de naissance, mais également le mot de passe par défaut, composé de quatre zéros. N'importe, je dis bien n'importe, quelle combinaison est plus sécurisée. L'autre mesure qui peut être intéressante, c'est désactiver sa boite vocale. Au fond, il n'y a rien de mieux à faire si vous ne souhaitez pas que quelqu'un puisse accédez à des messages que l'on vous laisse.

Cependant, je crois que sur des questions de sécurités, celle-ci est parmi les plus négligeables. En vérité, l'accès au téléphone en tant que tel est autrement plus préoccupant que l'accès à la boite vocale, et les révélations d'Edward Snowden ont démontré que plusieurs services gouvernementaux peuvent avoir accès à l'intégralité des fonctionnalités d'un téléphone. Y compris les plus étranges, comme la puce "baseband" de Samsung qui permet d'effacer ou d'ajouter des contenus sur une carte. Pratique quand on veut accuser quelqu'un de pédopornographie, par exemple. C'est, à mon sens, une situation bien plus inquiétantes d'autant plus que nous stockons de plus en plus d'informations via nos téléphones. Et il ne s'agit pas simplement de problème de sécurisés, mais de failles introduites volontairement, pour permettre à ces services d'accéder aux données.