07.05.2026

SMS Blaster : une nouvelle arnaque arrive en Suisse

La Suisse est actuellement frappée par une nouvelle forme de cyberattaque particulièrement sournoise, faisant intervenir un dispositif spécial appelé « SMS Blaster ». Cet équipement permet aux escrocs d'envoyer des messages frauduleux aux smartphones situés à proximité, sans même connaître leur numéro de téléphone, ni passer par le réseau des opérateurs classiques.

D'un point de vue technique, le dispositif fonctionne comme une antenne-relais de téléphonie mobile. Il émet un signal si puissant que les smartphones situés dans un rayon de quelques centaines de mètres s'y connectent automatiquement. Une fois la connexion établie, les appareils basculent momentanément sur le réseau 2G, aujourd'hui largement obsolète. Or ce sont précisément les vulnérabilités du réseau 2G qu'exploitent les escrocs pour faire parvenir leurs messages SMS aux téléphones connectés, contournant ainsi les filtres de sécurité des opérateurs.

D'ailleurs, ces faux messages sont souvent d'un réalisme bluffant. Pour plus de crédibilité, ils semblent souvent provenir d'autorités officielles, de banques ou de services de livraison, et contiennent généralement un lien vers un site frauduleux. L'objectif est, comme toujours, d'inciter les victimes à saisir des données confidentielles, telles que leurs numéros de carte bancaire ou leurs identifiants de connexion à l'e-banking. La force de ce type d'attaque réside aussi dans la possibilité d'adapter le contenu des messages des messages au contexte local. Ainsi, dans une zone de parkings payants, les escrocs peuvent envoyer des messages signalant une prétendue amende de stationnement.

Mais l'aspect le plus critique réside dans le fait que ces attaques court-circuitent les canaux de communication habituels. En effet, si les SMS de phishing traditionnels sont de plus en plus souvent détectés par les systèmes de filtrage des opérateurs, ceux envoyé via un SMS Blaster passent complètement sous les radars. Enfin, c'est un procédé qui offre aux criminels une grande liberté d'action. Ces derniers peuvent en effet se déplacer partout, cibler des lieux stratégiques et multiplier les tentatives autant de fois qu'ils le souhaitent. Et comme la grande majorité des smartphones continuent de prendre en charge la 2G, les faux messages parviennent aussi aux modèles de téléphone les plus récents.

Il est toutefois important de noter que cette menace ne concerne que les SMS classiques qui utilisent la connexion au réseau mobile. Les messageries instantanées fonctionnant via Internet, tels que WhatsApp, Signal ou Telegram ne sont donc pas concernées par les attaques par SMS Blaster.

Mesures de prévention

Voici les bons réflexes à adopter pour se prémunir contre ce type d'arnaque :

- ne cliquez pas sur les liens contenus dans des SMS suspects ou non sollicités ;
- saisissez toujours manuellement l'adresse des sites web des banques, administrations ou prestataires de services dans votre navigateur, ou utilisez l'application mobile officielle ;
- ne saisissez jamais de données confidentielles, telles que vos numéros de carte bancaire ou vos identifiants sur

des sites vers lesquels vous avez été redirigé par SMS.

- Si votre appareil le permet, désactivez le réseau 2G.
  - Sur Android : beaucoup d'appareils permettent de désactiver la 2G dans les paramètres, généralement sous « Réseau et Internet ».
  - Sur iPhone : Apple ne permet pas de désactiver spécifiquement le réseau 2G. L'alternative consiste à activer le « mode isolement » (dans « Confidentialité et sécurité »), sachant que cela peut également limiter certaines fonctionnalités de l'appareil.
- Supprimez systématiquement les SMS douteux et signalez-les systématiquement (sur www.antiphishing.ch (https://www.antiphishing.ch) par exemple).
- En cas de doute, contactez directement l'organisme prétendument à l'origine du message en utilisant ses coordonnées officielles.