Manuel du parfait pirate GSM

- Technologie -

Date de mise en ligne : jeudi 6 octobre 2005

Spyworld Actu

Comment exploiter les nombreuses failles du réseau téléphonique cellulaire ? Quatre chercheurs de la Penn State University viennent de publier un mémoire expliquant les différentes phases d'une attaque en déni de service conduite à l'aide d'une avalanche de SMS. L'étude elle-même et le communiqué explicatif détaillent comment bloquer une cellule ou toute une zone géographique, en engorgeant de « Texto » des infrastructures qui, parfois, ne peuvent acheminer plus de 110 messages par seconde. Cette analyse repose essentiellement sur des mesures pratiquées sur le réseau cellulaire américain. Mais point n'est besoin d'effet 11 septembre pour se rendre compte qu'un réseau d'opérateur peut s'écrouler sous une forte demande. Un 15 août sur la côte d'Azur ou un salon télécom à Paris-Porte de Versailles (à l'heure du déjeuner) l'enseigne à tout usager en mal de communication.

L'analyse technique de ces universitaires rappelle plus ou moins des travaux similaires que l'on faisait il y a 15-20 ans. Une époque où l'on regardait de près la QoS des réseaux Ethernet, et où l'on affirmait que jamais une ligne téléphonique ne passerait le cap des 2400 bps. Mais ces scientifiques ont su largement dépasser le simple examen de bande passante. L'article déborde notamment sur les autres menaces qui planent sur les réseaux GSM. Des menaces plus concrètes, plus immédiates, précisent les auteurs. A commencer par le googlehacking de numéros de cellulaires -aisément transposable en France-, le potentiel extraordinaire des réseaux de téléphonie mobile en matière de spamming, l'augmentation très nette d'attaques en phishing via SMS mesurées depuis ces dernières années, et la croissance très probable d'infections virales. Etrangement, les quatre chercheurs ne tentent pas à approfondir ces axes de développement. Pour l'heure, seuls quelques chasseurs de virus très spécifiques, tel F-Secure, bataillent pour attirer l'attention des opérateurs sur ce phénomène. Hélas, le discours est celui d'un éditeur d'A.V. traditionnel : alarmiste, techniciste, focalisé sur la dernière attaque connue. Pourtant, point n'est besoin d'être spécialiste pour deviner ce qui risque d'arriver.

Chaque jour qui passe voit son lot de SMS de phishing et de Social Engineering : messages bancaires bidons, demandes de rançons, propositions commerciales douteuses, pseudo « confidences communiquées par erreur »... ces pratiques sont monnaie courante au Moyen Orient et dans les pays du Sud Est asiatique. En France, sur ces sujets, nos opérateurs observent un mutisme préoccupant. Préoccupant, car non seulement il sera trop tard pour lancer des campagnes de sensibilisation lorsque cette nouvelle forme de criminalité frappera les relais français, mais en outre il faut s'attendre d'ici là à ce que les techniques virales « Symbian based » ou « Dot Net aware » aient fait de sérieux progrès. Peut-on réellement croire que le phishing sur cellulaire sera plus propre que celui véhiculé par messagerie ? C'est peu probable. L'attaque téléphonique de demain a de très fortes chances d'être accompagnée des mêmes infections que nos boîtes à lettres d'aujourd'hui : keyloggers compatibles T9, récolteurs d'agendas et de numéros téléphoniques -les adress harvester du futur-, noyaux de « zombification » chargés de transformer un cellulaire en réémetteur de SMS et MMS de spam/spywares... Il serait peut-être temps que l'on cesse de se focaliser sur Cabir et que l'on envisage sérieusement les risques de développement d'une telle cohorte de menaces. Ce « On » chargé d'envisager ne saurait relever uniquement des opérateurs, pour d'évidentes raisons de conflits d'intérêts et d'absence d'objectivité. En outre, les premiers virus du genre l'ont prouvé, si certaines attaques peuvent provenir du réseau MMS (ainsi Mabir), d'autres n'ont nul besoin d'utiliser les canaux des opérateurs (Virus Bluetooth, et pourquoi pas WiFi...). Enfin, rien n'interdit non plus de réinventer d'anciennes techniques d'infection, généralement invisibles aux yeux des A.V., telles que l'émission de codes en « covert channel » ou l'expédition de malwares fragmentés en multiples SMS apparemment innocents.

Ce n'est pas là une vision apocalyptique du « digital chaos ». La planète Internet continue de tourner avec le phishing, les virus, le spam... mais moins bien. Le monde de la téléphonie cellulaire lui aussi continuera de tourner, mais moins bien si l'on n'y prend garde.