

Phishing : la police française s'appuie sur le secteur privé

La plate-forme Pharos, créée par la Police Nationale en 2009 pour recueillir et traiter les signalements de contenus ou comportements illicites sur Internet, se rapproche de la Phishing Initiative, une association créée en 2011 à l'initiative de Microsoft, Paypal et la PME française spécialiste de cybersécurité Lexsi pour lutter contre le hameçonnage (ou phishing). **Catherine Chambon** (à gauche sur la photo ci-dessus), la sous-directrice chargée de la lutte contre la cybercriminalité à la DCPJ (Direction centrale de la Police Judiciaire), et **Jérôme Robert**, le directeur marketing de Lexsi qui préside par ailleurs la Phishing Initiative, viennent de signer une convention de partenariat. Principal objectif : le partage d'informations entre Pharos et la plate-forme animée par l'association anti-hameçonnage, plate-forme qui alimente les listes noires utilisées au sein des principaux navigateurs Web (Chrome, Firefox, Internet Explorer et Safari).

« Pharos vise à mettre en branle le travail de police, explique Jérôme Robert (en photo ci-contre). Alors que la Phishing Initiative a pour objectif de bloquer rapidement les URL frauduleuses. L'association des deux va permettre de protéger les particuliers tout de suite, pendant le temps de l'enquête. De côté de la Phishing Initiative, nous sommes intéressés par les volumes de signalements qui transitent par Pharos, car nous avons pour but de faire tomber des campagnes entières, impliquant parfois plusieurs URL. Nous visons donc l'exhaustivité. » Selon le directeur marketing de Lexsi, l'échange de données entre les deux plateformes sera en place d'ici à la fin de l'année. En sus, les deux partenaires comptent sur leur association pour mieux informer le grand public des risques du phishing, via la production de rapports périodiques sur le sujet.

Temps réel pour les menaces importantes

« Une attention tout particulière sera donnée aux modes opératoires affectant des organisations françaises et aux contenus illicites rédigés en français ou hébergés en France. D'autre part, Phishing Initiative alertera la SDLC (Sous-direction de la lutte contre la cybercriminalité, NDLR) en temps réel des campagnes de phishing d'une ampleur significative ou en forte progression », précise la convention signée cette semaine par les deux parties. Chaque partenaire s'engage par ailleurs à référencer les outils de signalement de l'autre.

Selon Catherine Chambon, 137 000 signalements d'escroqueries par Internet ont été répertoriés sur Pharos en 2014, dont un tiers liés à des techniques de phishing. De son côté, la Phishing Initiative dit avoir reçu 60 000 signalements depuis le début d'année, qui ont abouti à répertorier 35 000 URL employées par les spammeurs.

Opérée par Lexsi, qui y dédie des ressources humaines, la plate-forme Phishing Initiative cible le phishing de masse visant le grand public, et non le spearphishing (hameçonnage ciblé dont sont souvent victimes les entreprises). « Mais de nombreuses entreprises se servent de la plate-forme pour effectuer des signalements quand leur marque est usurpée », explique Jérôme Robert. Elles bénéficient dès lors de la protection offerte par l'association (placement sur les listes noires de Microsoft et Google – cette dernière étant également exploitée par Firefox et Safari -, fermeture des URL

concernées). Face à ce phénomène, Lexsi envisage désormais de proposer de nouveaux services payants à ces sociétés, comme l'envoi d'URL sous forme de flux. Une façon d'équilibrer les comptes de l'association et de ne pas cannibaliser l'activité de Lexsi, qui vend par ailleurs des services de protection contre le hameçonnage.

A lire aussi :

[FIC 2015 : les hackers ont gagné une bataille, pas la guerre](#)

[Après les attentats : l'Intérieur bricole un plan d'action, pas un Patriot Act](#)

Crédit photo : Ministère de l'Intérieur/DICOM/P.CHABAUD