« Les cyberattaques peuvent toucher Marcoule »

Entretien | Jean-Paul Pinte, expert en cybercriminalité, donnera une conférence au Visiatome.

À l'occasion de sa venue au Visiatome de Marcoule, le 17 novembre, Jean-Paul Pinte, maître de conférences en sciences de l'information et de la communication à l'université catholique de Lille, spécialiste de la cybercriminalité et cybercriminologue, explique les dangers de cette nouvelle menace pour des sites sensibles.

■ Les sites sensibles, comme Marcoule sont, toujours soumis des dangers de cyberattaques.

En quoi, votre intervention est significative pour le site de Marcoule ?

Aujourd'hui, la cybercriminalité évolue et de nouvelles tendances se dessinent avec des modes opératoires sophistiqués.
Les entreprises, petites ou grandes, tout comme les grands groupes ou les sites stratégiques sont susceptibles d'attaques virales.

Comment se matérialise ce danger virtuel ?

Une forme très répandue de cybercriminalité est connue sous le nom "d'ingénierie sociale", en anglais, on parle de *social engineering*. Ce terme désigne l'art de manipuler les personnes afin de contourner des dispositifs de sécurité. Il s'agit ainsi d'une technique consistant à obtenir des informations de la part des utilisateurs par téléphone, courrier électronique, courrier traditionnel ou contact direct.

Qui se cache derrière cette forme de criminalité ?

Du pirate ou hacker solitaire, nous avons aujourd'hui à faire face à des groupes de plus en plus organisés et capables d'immobiliser un système informatique, voire de le paralyser pour retirer une rançon, connue sous le nom de "kidnapping and ransom" (lire ci-contre).
À noter que l'utilisation de ransomwares a été la pratique la plus courante au cours de l'année 2016.

Même des sites extrêmement sécurisés comme des centrales nucléaires peuvent être infectés ?

Oui ! Actuellement, rien n'est inattaquable aujourd'hui.
Des opérateurs d'importance vitale (OIV) les centrales nucléaires, la distribution de l'eau du gaz, du pétrole ou de l'électricité sont des cibles à ne pas négliger.
Par exemple, le virus Stuxnet avait été introduit au moyen d'un périphérique USB au cœur d'une des centrales atomiques russes. Cette attaque est devenue une référence dans le monde des cybercriminels et a même permis d'améliorer leur technique. Une fois l'existence de Stuxnet connue, les pirates à travers le monde se sont inspirés de son fonctionnement et ont incorporé certaines de ses fonctionnalités à leurs propres logiciels à visée malveillante. La communauté nucléaire commence à s'en inquiéter. L'Agence internationale de l'énergie atomique (AIEA) qui s'est réunie à Vienne, en juin dernier, avec 650 experts de 92 pays a émis le souhait d'une collaboration avec Interpol. Une première réalisation a d'ailleurs été faite.

Que doivent alors faire ces industries ?

Face à l'augmentation en quantité et en sophistication des attaques informatiques, et à leurs impacts potentiellement destructeurs, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a pour mission d'accompagner les opérateurs d'importance vitale dans la sécurisation de leurs systèmes d'information sensibles. Pour parer les tentatives d'attaques les opérateurs d'importance vitale devront garder des traces des incidents de sécurité dont ils sont victimes afin d'avoir un certain recul et des bases de données sur ces attaques. Mais tout le problème est que ces traces sont classées confidentielles…

PIERRE-JEAN CÔME
pcome@midilibre.com

REPÈRE

Une bonne terminologie

Les attaques sur le web peuvent se faire de plusieurs façons. Les plus connus sont l'hameçonnage ou *phishing* et le "rançongiciel" ou *ransomware*.
L'hameçonnage est une technique courante. L'objectif : opérer une usurpation d'identité afin d'obtenir des renseignements personnels et des identifiants bancaires pour en faire un usage criminel. Le cybercriminel se « déguise » en un tiers de confiance (banques, administrations, fournisseurs d'accès à internet…) et diffuse un mail frauduleux, ou contenant une pièce jointe piégée, à une liste de contacts. Ces informations sont alors mises à disposition du cybercriminel qui n'a plus qu'à faire usage des identifiants, mots de passe ou données bancaires récupérés.
Les « rançongiciels », eux, sont des programmes informatiques malveillants de plus en plus répandus (ex : Locky, TeslaCrypt, Cryptolocker). L'objectif : chiffrer des données puis demander à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.
Le cybercriminel diffuse un mail qui contient des pièces jointes et/ou des liens piégés. Le corps du message contient un message rédigé qui demande de payer rapidement une facture par exemple. Les fichiers devenus inaccessibles, un message s'affiche pour réclamer le versement d'une rançon, payable en bitcoin ou *via* une carte prépayée, en échange de la clé de déchiffrement.
Rien n'indique que le déchiffreur en question soit efficace.

Deux radars mobiles détruits par les flammes

Faits divers | Les appareils situés sur la RN 86 et la RD 6 ont été volontairement brûlés.

Même pas un mois… Le radar mobile autonome installé le 10 octobre, sur la RN 86, côte de Roquebrune, lors de l'opération de contrôle d'enverguere, supervisée par le préfet du Gard, est parti en fumée, dans la nuit de samedi 5 au dimanche 6 novembre. De plus, il semblerait qu'au cours de la même période, le dispositif de contrôle de vitesse, positionné sur la RD 6, à hauteur de la commune de Colombier ait subi le même sort… Appelés dans la nuit, les gendarmes de la compagnie de Bagnols-sur-Cèze ont constaté les faits.

■ Les radars mobiles récemment déployés sur les routes du Gard rhodanien semblent gêner. Photos P.-J. C.

■ Des dégâts irréversibles ont été causés.

Matière inflammable

Selon nos informations, un radar est en zone gendarmerie, l'autre en zone police. C'est cette dernière qui est en charge de l'enquête qui a débuté. Les deux radars ne sont plus que des amas de tôle noircis par les flammes. Lorsque l'on s'approche des deux carcasses calcinées, il est possible d'apercevoir une traînée noirâtre laissée par les flammes. À première vue, une matière inflammable aurait été utilisée afin de propager l'incendie sur les structures métalliques. À noter que les capots renfermant les instruments gérant l'électronique ont été forcés. Au début de cette semaine, un autre radar mobile autonome, installé sur la RN 580, aux portes de Bagnols-sur-Cèze avait été détérioré au moyen de peinture occultant la focale qui flashe les véhicules en excès de vitesse. L'ensemble de ses dispositifs de contrôle de vitesse ont été souhaités par la préfecture du Gard afin d'endiguer le nombre grandissant de tués sur les routes du Gard rhodanien depuis le début de l'année.

PIERRE-JEAN CÔME
pcome@midilibre.com