Airbus déjoue douze attaques informatiques majeures par an

	Airbus déjoue douze attaques informatiques majeures par an

Le chiffre a de quoi inquiéter pour les sus-listiles. Airbus Group, la maison mère de l'aéronomer toulousain, subit chaque année des milliers de cyberattaques en provenance du monde entier.

Parmi ce flot, seule une dauzaine sont jugées vraiment «sérées» par Stéphane Lenco, le directeur de la sécurité informatique du géant de l'aéronactique et de la défense. Airbus Group et ses divisions doivent faire face à deux grands types d'attaques informatiques : contre son propre réseau d'information d'abord (internet, intranet, serveurs…) et contre ses produits, c'est-à-dire contre l'intelligence embarquée à bord de ses avions, ses satellites, ses missiles, etc.
Parmi ces attaques se cachent certains groupes obcrtés par des «tats». Ce fut le cas lorsqu'en 2013 un groupe sclitrate chinois est parvenu à pénétrer les réseaux du New York Times grâce à une série d'e-mails d'hameçonnage et à des logiciels malveillants (malwares) mis au point spécialement pour cette intrusion. «Les motivations de ce type de pirates peuvent être multiples. Ils peuvent rechercher un accès à des brevets, à des propositions commerciales usire à la messagerie des top managers allant jusqu'au MDS» confie une source interne à Airbus Defence and Space spécialiste de la cybersécurité.
Mais pour des industriels comme Airbus le principal danger reste les actions de sabotage qui viseraient à ralentir ou perturber la production d'avions par exemple.
Une variante de ce type d'attaque consiste aussi à réclamer une rançon afin par exemple de donner une clef informatique indispensable pour décrypter des fichiers que les pirates ont encryptés. «Airbus s'est pas directement visé par ce type d'attaque mais elles connaissent une énorme explosion actuellement auprès des industriels» a souligné le patron de la sécurité d'Airbus Group au cours d'une récente conférence en Australie.

145 000 employés, autant de portes d'entrée

Il ne cître l'exemple de cet employé d'un sous-traitant d'Airbus qui à vu ses fichiers de son ordinateur se crypter alors qu'il se connectait au réseau de l'entreprise étendue d'Airbus. Il s'agit d'un extranet qui permet aux fournisseurs d'Airbus de dialoguer, d'échanger des documents, de livrer des plans,etc. avec leur donneur d'ordres.
Grâce à l'action des services de sécurité d'Airbus, cette attaque a pu être déjouée dans les deux heures et les sauvegardes activées. Ainsi, ni les opérations d'Airbus ni les données de ses recherches n'ont été attaintes.
C'est bien l'un des problèmes du groupe aéronautique. Il compte 165 sites dans 36 pays et 145 000 employés dans le monde. «Ce sont autant de portes d'entrée qu'il faut sécuriser même si les pirates ne ciblent pas tout le monde mais seulement les plus intéressants ou les plus vulnérables» analyse un expert de la cyber-sécurité.
«La sonde Keelback Net permet aux cyber experts d'Airbus DS à Élancourt de détecter 24 heures sur 24, 7 jours sur 7, dans le réseau du client toute trace ou comportement suspects, en particulier les signaux faibles confie le responsable d'Airbus Defence and Space». Il faut en effet agir vite pour éviter ou limiter les dégôts de ces intrusions malveillantes. Ainsi Airbus D & S a mis au point Keelback Net qui détecte le plat en amont possible les cyber-menaces persistantes avancées (Advanced Persistent Threats en anglais APT) qui sont les plus dangereuses car les plus difficilement détectables.
Le but d'une attaque APT est de s'installeire dans un ordinateur susceptible de contenir des informations de valeur ou, s'il n'en détient pas, qui peut se transformer en passerelle pour atteindre un ordinateur plus intéressant. Les pirates peuvent ainsi installer un enregistrmur de frappes qui lit tout ce que le clavier tape ou bien créer une porte dérobée (backdoor) sur l'ordinateur d'un employé lambda qui est connecté sur le même réseau que les ordinateurs qui contiennent, eux, des données importantes.

Aucun hacker n'est embauché chez Airbus

Face à ces attaques qui se multiplient depuis cinq ans, Airbus Group a réagi en mobilisant des budgets importants. «Quand le patron (Tom Enders) vous donne de l'argent, il veut des résultats» a lancé Stéphane Lenco. Mais il concède qu'il y a encore des progrès à faire.
Pour mener à bien ses projets ou devoir, ces spertain d'embaucher des hackers chez Airbus pour acquérir plus vite cette nouvelle façon de penser. Ce n'est pas la philosophie, du moins officielle, du géant de l'aéronautique.
Sur le terrain, des réunions régulières rappellent aux salariés d'Airbus les précautions à prendre comme ne pas laisser traîner des clefs USB qui pourraient alors embarquer un logiciel espion si elles tombaient dans des mains mal intentionnées.

Une division spéciale de 600 experts

C'est à Élancourt dans les Yvelines qu'Airbus Defence and Space abrite une branche entière dédiée à la cybersécurité. Créée en 2011 elle concentre 600 experts répartis entre la France, l'Allemagne et le Royaume-Uni. Ces compétences particulières sont utilisées tant au sein même d'Airbus Group que pour des clients externes comme les gouvernements, les infrastructures critiques et les grandes entreprises stratégiques. En décembre dernier, Airbus DS a ainsi été choisie par TVS Monde pour sécuriser son système d'information suite à la cyber attaque subie par la chaîne le 8 avril 2015 et qui avait paralysé l'antenne. Autre client de marque : les forces armées françaises pour lesquelles Airbus DS déploie un système de lutte informatique défensive qui identifie les cyber attaques, rétrogère les éléments de contexte de chacune d'entre elles (origine, destination, criticité et impact) et les combat dans le cadre d'un plan de «réaction». Airbus DS capitalise sur cette expérience auprès des militaires pour améliorer sa gamme de services qui sont ensuite proposés à des clients civils. «Airbus DS CyberSecurity investit 20 % de son chiffre d'affaires dans la recherche et développement (R & D) pour rester «up to date»… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (vols, espionnages, piratages, fraudes, arnaques Internet,...) et judiciaires (investigations téléphones, disques durs, e-mails, contrefaçons, conflits client-fournisseur,...)
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Contactez-nous

Réagissez à cet article

Source : *Piratage informatique : Airbus déjoue douze attaques majeures par an — 06/05/2016 — ladepeche.fr*

article de Gil Bousquet