# Plusieurs escrocs sur Leboncoin écopent de peines de prison


Plusieurs escrocs sur Leboncoin écopent de peines de prison

**Les autorités utilisent Leboncoin pour surveiller les escrocs qui revendent du matériel volé. Plusieurs forces de police indiquent avoir réussi à arrêter des auteurs présumés, certains ont même été condamnés à des peines de prison.**


Comme bon nombre de plates-formes de vente en ligne, Leboncoin.fr peut servir pour des escrocs de moyen d'écouler une marchandise indûment obtenue voire d'appâter des victimes. En région parisienne, un groupe de personnes vient d'être condamné à des peines de prison pour avoir revendu des voitures sur le site.
Ces véhicules d'occasion étaient achetés avec de faux chèques de banque pour les revendre, 30 à 40 % moins cher que l'argus, contre des espèces. Des annonces étaient régulièrement publiées sur Leboncoin puis rapidement retirées, une fois la vente conclue. Au total, 71 automobiles ont été répertoriées par les forces de police.
Selon Le Parisien, les escrocs ont pu être repérés notamment grâce aux annonces publiées sur le site.
Le cerveau du réseau, un homme de 28 ans, écope d'une peine de 5 années de prison dont 1 an avec sursis avec mise à l'épreuve. Il devra en outre rembourser les victimes. Les autres membres ont été condamnés par le tribunal correctionnel de Pontoise à 4 et 2 ans de prison (associées à des peines de sursis).

**Le site internet leboncoin.fr**

Un voleur arrêté après avoir mis des annonces sur Leboncoin
En Bretagne, les autorités indiquent avoir interpellé un homme soupçonné d'avoir dérobé du matériel de jardinage auprès d'une enseigne locale. L'individu a volé des objets pour un préjudice total estimé à 2 500 euros puis a tenté de revendre une partie du butin sur Leboncoin, sans se soucier que le vendeur ou la gendarmerie surveillerait la plate-forme.
Dans les jours suivants le délit, le responsable du magasin qui avait subi le vol a trouvé une annonce pertinente. « Nous avons ensuite travaillé à partir de cette annonce, puis nous sommes remontés jusqu'à l'auteur présumé des cambriolages », explique le maréchal des logis-chef Goby auprès du quotidien Ouest-France.
Le domicile de la personne a été perquisitionné et nombre d'objets dérobés s'y trouvaient. L'affaire a été transmise au parquet de Brest, où sera jugé l'auteur présumé.

---

Réagissez à cet article

Source : *Plusieurs escrocs sur Leboncoin écopent de peines de prison*

---

# Critical Infrastructure Sectors of Nations facing cybercrime


Critical Infrastructure Sectors of Nations facing cybercrime

---

**There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.**

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7.
PPD-21 identifies 16 critical infrastructure sectors:

**Chemical Sector**
The Department of Homeland Security is designated as the Sector-Specific Agency for the Chemical Sector.

**Commercial Facilities Sector**
The Department of Homeland Security is designated as the Sector-Specific Agency for the Commercial Facilities Sector.

**Communications Sector**
The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government.

**Critical Manufacturing Sector**
The Department of Homeland Security is designated as the Sector-Specific Agency for the Critical Manufacturing Sector.

**Dams Sector**
The Department of Homeland Security is designated as the Sector-Specific Agency for the Dams Sector. The Dams Sector comprises dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, and other similar water retention and/or control facilities.

**Defense Industrial Base Sector**
The Defense Industrial Base Sector is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements.

**Emergency Services Sector**
The Department of Homeland Security is designated as the Sector-Specific Agency for the Emergency Services Sector. A system of prevention, preparedness, response, and recovery elements, the Emergency Services Sector represents the nation's first line of defense in the prevention and mitigation of risk from terrorist attacks, manmade incidents, and natural disasters.

**Energy Sector**
The U.S. energy infrastructure fuels the economy of the 21st century.

**Financial Services Sector**
The Department of Treasury is designated as the Sector-Specific Agency for the Financial Services Sector.

**Food and Agriculture Sector**
The Department of Agriculture and the Department of Health and Human Services are designated as the Co-Sector-Specific Agencies for the Food and Agriculture Sector.

**Government Facilities Sector**
The Department of Homeland Security and the General Services Administration are designated as the Co-Sector-Specific Agencies for the Government Facilities Sector.

**Healthcare and Public Health Sector**
The Department of Health and Human Services is designated as the Sector-Specific Agency for the Healthcare and Public Health Sector.

**Information Technology Sector**
The Department of Homeland Security is designated as the Sector-Specific Agency for the Information Technology Sector.

**Nuclear Reactors, Materials, and Waste Sector**
The Department of Homeland Security is designated as the Sector-Specific Agency for the Nuclear Reactors, Materials, and Waste Sector.

**Transportation Systems Sector**
The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.

**Water and Wastewater Systems Sector**
The Environmental Protection Agency is designated as the Sector-Specific Agency for the Water and Wastewater Systems Sector.

---

Réagissez à cet article

Source : *Critical Infrastructure Sectors | Homeland Security*

---

# Panne électrique en Ukraine : le malware aurait été aidé par l'humain


Panne électrique en Ukraine : le malware aurait été aidé par l'humain

---

 **Le mois dernier, une cyberattaque contre des fournisseurs d'énergie ukrainiens avait privé 80 000 clients d'électricité. D'après la signature du malware, l'attaque avait été imputée à un groupe de pirates ayant des liens avec la Russie. Mais, selon une nouvelle étude, le malware n'est pas directement à l'origine de la panne : les assaillants sont intervenus physiquement pour activer les disjoncteurs et provoquer la coupure de courant.**

Selon des informations publiées samedi par l'équipe du SANS Industrial Control Systems (ICS), une organisation spécialisée dans l'information et la formation des professionnels de la sécurité, le malware a bien servi aux pirates à s'introduire dans le réseau des fournisseurs d'électricité, mais ils sont ensuite intervenus sur les disjoncteurs pour couper l'alimentation. Depuis des années, les experts mettent en garde sur la vulnérabilité des systèmes de contrôle industriels. Les cyberattaques survenues le 23 décembre contre les installations ukrainiennes montrent que leurs craintes sont justifiées. Selon les experts du #SANS ICS, ces évènements sont aussi la preuve que de telles attaques sont planifiées et très coordonnées.
Depuis l'annexion de la Crimée par la Russie en 2014, les tensions entre la fédération et l'Ukraine restent fortes. « Pour masquer le piratage et l'intrusion dans les réseaux, les agresseurs sont intervenus physiquement sur la centrale électrique », a déclaré l'équipe du SANS ICS. « Les agresseurs ont également lancé en simultané une attaque DDoS par déni de service sur le réseau téléphonique afin de bloquer les appels des clients affectés par la panne », a encore déclaré l'organisation. Les attaques auraient visé les deux fournisseurs d'énergie Prykarpattyaoblenergo et Kyivoblenergo. Ce dernier a déclaré dans une mise à jour de service que 80 000 clients dépendant de 30 sous-stations avaient été déconnectés du réseau.

## Des pannes provoquées par une action physique

Plusieurs entreprises de sécurité ont analysé le #malware Black Energy 3 et le #composant Killdisk utilisés pour les attaques. Jeudi dernier, l'entreprise de sécurité iSight Partners basée à Dallas a déclaré que ces logiciels malveillants avaient déjà été utilisés dans le passé par le #groupe de pirates Sandworm connu pour avoir de puissants intérêts russes. Mais, comme iSight, le SANS ICS pense que les pannes ne sont pas à mettre exclusivement sur le compte des malwares. « Autrement dit, de nouvelles preuves pourraient remettre en cause l'impact réel des composantes malveillantes impliquées dans l'attaque », a écrit Michael Assante, directeur du SANS ICS.
Le composant Killdisk écrase le Master Boot Record (MBR), premier secteur du disque dur chargé par le PC avant de monter le système d'exploitation, et empêche donc le PC de démarrer. Selon Symantec, Killdisk peut aussi écraser des fichiers en écrivant des données inutiles. Michael Assante avance que Killdisk n'était pas compatible avec le système SCADA de contrôle et d'acquisition de données utilisé par les deux opérateurs. Mais il a peut-être été utilisé pour effacer d'autres fichiers qui auraient permis la restauration des systèmes. « Il semble que les fournisseurs d'électricité ont rétabli leurs services en actionnant manuellement les disjoncteurs au bout de trois et six heures », a ajouté le directeur du SANS ICS. Selon lui, « il faudrait féliciter les opérateurs ukrainiens pour leur diligence et les efforts accomplis pour restaurer leurs services ».

---

Réagissez à cet article

Source : *Panne électrique en Ukraine : le malware n'est pas seul en cause – Le Monde Informatique*

# FIC 2016 les 25 et 26 janvier 2016 sur le thème de la sécurité des données

| | |
|---|---|
|  | #FIC 2016 les 25 et 26 janvier 2016 sur le thème de la sécurité des données |

**Pendant longtemps, la sécurité des données se confondait avec celle de la sécurité des systèmes d'information. Or la décorrélation croissante entre le contenant (support physique ou applicatif) et le contenu en raison de l'émergence des technologies de virtualisation, du « cloud computing » et de nouveaux modèles économiques change aujourd'hui la donne. La donnée est devenue un « objet » à part entière qui s'appréhende indépendamment de son support.**

## Axe 1 : les données, carburant de la transformation numérique.

Les données sont omniprésentes et multiformes : on peut citer les données personnelles, sociales, médicales, bancaires, d'entreprises, de géolocalisation, de sécurité, de dossiers passagers (PNR) etc. Cette compartimentation en fonction des usages ou des secteurs d'activité a-t-elle cependant encore un sens ? Comment gérer l'information indépendamment des supports utilisés ? Au-delà de la métaphore, les données constituent-elles véritablement un « nouvel or noir » ?

## Axe 2 : la maitrise des données, enjeu de souveraineté

Posséder une « industrie de la donnée » puissante est un atout essentiel dans la compétition mondiale et une composante importante de toute stratégie de puissance. Or l'Europe apparait de ce point de vue en net retrait par rapport aux Etats-Unis. Forte consommatrice de numérique, la faiblesse de son offre locale la conduit à exporter massivement ses données, principalement aux Etats-Unis. Comment passer d'une « Europe offerte » à une Europe « ouverte » ? Quelle est la situation des autres continents ? Peut-on parler de « géopolitique des données » ?

## Axe 3 : les données, un capital menacé

Si les attaques en déni de service visent les infrastructures elles-mêmes, les données sont souvent l'objectif ultime des attaquants, qu'il s'agisse de cybercriminalité (vol d'information, crypto-locking…) ou d'espionnage. Quelles sont les dernières tendances observées ? Quels sont les modes opératoires des cybercriminels ? Comment calculer la valeur de ses données pour engager des poursuites ?

## Axe 4 : droit et données

La donnée est une notion immatérielle qui soulève de nombreuses questions au plan juridique. Peut-on appliquer la notion de propriété à la donnée, notamment à la donnée personnelle ? Quel lien entre données et territoire ? Comment mettre en œuvre efficacement le droit à l'oubli aujourd'hui consacré dans certains pays ? Comment définir le vol de données au plan pénal ?

## Axe 5 : quelles stratégies de sécurité des données pour l'entreprise ?

Pour les entreprises, la sécurité des données repose sur une approche globale impliquant : classification des données, évaluation des données, analyse de risques, définition et mise en œuvre d'une stratégie de sécurité. Le développement du cloud computing et l'externalisation croissante de l'IT soulèvent à cependant de nombreuses questions. Peut-on utiliser « en toute sécurité » un CRM ou un ERP dans le Cloud ? Quelles conséquences en termes de maîtrise des données ? Comment assurer les risques liés aux données ?

## Axe 6 : quelles technologies pour sécuriser les données ?

Le responsable sécurité des systèmes d'information dispose aujourd'hui d'une vaste bibliothèque d'outils et de technologies lui permettant de sécuriser ses données, qu'il s'agisse d'outil de protection, de destruction sécurisée, de détection de fuites d'information ou d'investigation. La vitesse du progrès technologique et le « time to market » imposé par le marché aux éditeurs sont-elles compatibles avec les cycles d'adoption relativement lents des organisations ? Compte tenu de ce même « time to market », comment intégrer la sécurité de façon native (security by design) dans les applications à disposition des utilisateurs ?

## Axe 7 : données et enjeux sectoriels

La transformation numérique et les données qui la nourrissent irriguent l'ensemble des secteurs économiques et des activités humaines. Les données sont ainsi au cœur de la « smart revolution » qui touche aussi bien l'individu dans sa vie quotidienne, la collectivité ou l'entreprise au travers des objets connectés et de « l'informatique omniprésente ». Quels sont les enjeux liés aux données dans la « ville intelligente », « l'usine du futur », le monde médical etc. ?

## Axe 8 : enjeux sociétaux et éthiques liés aux données.

La transformation numérique, et la croissance exponentielle des données qu'elle génère, constituent à n'en pas douter des opportunités. Mais la rapidité de cette évolution et ses conséquences majeures sur l'Homme militent également pour une certaine prise de recul et un questionnement éthique et philosophique. Au plan individuel, que signifie désormais la notion de « vie privée » ? Est-il également possible de replacer l'utilisateur au cœur de cette transformation en lui permettant de se réapproprier « ses » données ? Faut-il enfin imaginer, sur le modèle de la loi bioéthique, une loi sur l'éthique numérique fixant un cadre pour l'exploitation des données à des fins prédictives ou à des fins de surveillance ?

---

Réagissez à cet article

Source : *Le FIC 2016 aura lieu les 25 et 26 janvier 2016 sur le thème de la sécurité des données | Observatoire FIC*

---

# L’aviation civile n’est pas à l’abri du cyber-terrorisme

| | |
|---|---|
|  | L’aviation civile n’est pas à l’abri du cyber-terrorisme |

---

**A la demande de l'Agence européenne de sécurité aérienne (Aesa), un hacker pourvu d'une licence de pilote d'avion commercial a démontré qu'il pouvait en quelques minutes entrer dans le système de messagerie des compagnies maritimes.**

A l'instar des machines industrielles et des objets domestiques connectés, les véhicules et les avions n'échapperont pas aux attaques des cybercriminels. « L'aviation civile doit se préparer aux cyber-risques », prévient d'ailleurs Patrick Ky, le directeur exécutif de l'Agence européenne de sécurité aérienne (Aesa). En poste depuis 2013, ce dernier s'est exprimé lors d'un petit déjeuner organisé par l'association des journalistes de la presse aéronautique et spatiale (Aspae) en octobre dernier. Ses propos ont été rapportés dans de nombreux journaux tels que Les Echos, Le Parisien ou encore l'Usine Nouvelle. Patrick Ky est formel : le piratage informatique d'un avion est possible et la cybercriminalité représente bien une véritable menace pour le transport aérien.

Pour illustrer ses propos, le directeur exécutif de l'Aesa a confié qu'il avait fait appel à un Hacker. Cet expert en informatique – également titulaire d'une licence de pilote d'avion commercial – est parvenu en quelques minutes à entrer dans le système de messagerie Acars (Aircraft Communication Addressing and Reporting System) en se faisant passer pour un des administrateurs du réseau. Lequel sert aux compagnies aériennes à envoyer des messages automatiques et réguliers de l'avion vers le sol pour s'assurer du bon fonctionnement des systèmes critiques de l'avion.
Risque accru. Demain, le risque de cyberattaque va être accru avec la mise en place du système Sesar (Single European Sky ATM Research ; en français : Ciel unique européen) qui vise à harmoniser en Europe le trafic aérien en déployant un réseau et de nouveaux systèmes de gestion d'ici 2025. Ce nouveau réseau européen de contrôle du trafic aérien aura la possibilité de donner directement des instructions aux systèmes de contrôle de l'avion. Pour limiter les risques de piratage, l'agence européenne pourrait, à long terme, se charger de certifier les équipements contre les risques de cyberattaques sachant qu'elle a déjà la responsabilité de certifier les aéronefs en Europe. A court terme, Patrick Ky veut mettre en place une structure en charge d'alerter les compagnies aériennes sur les cyberattaques. Un risque sur lequel Air France, que nous avons contacté, ne s'est pas encore publiquement prononcé.

---

Réagissez à cet article

Source : *L'aviation civile n'est pas à l'abri du cyber-terrorisme*

# Les téléphones cryptés, le casse-tête des enquêtes antiterroristes


Les téléphones cryptés, le casse-tête des enquêtes antiterroristes

**Invité à s'exprimer sur France Inter, vendredi 8 janvier, sur les attentats qui ont frappé la France en 2015 et l'attaque, la veille, d'un commissariat du 18e arrondissement de Paris, le procureur de la République à Paris, François Molins, est revenu sur l'une des principales difficultés techniques à laquelle font face les enquêteurs en matière d'antiterrorisme : travailler sur les « téléphones cryptés » retrouvés, dont les codes de verrouillage sont de plus en plus complexes à casser.**


*« Tous les smartphones qu'on essaie aujourd'hui d'exploiter sont verrouillés et cryptés* (…) *toutes les communications passées par les terroristes sont passées à l'aide de logiciel de cryptage »*, a expliqué M. Molins, qui a cependant tu les noms des principaux logiciels utilisés.
*« Les évolutions technologiques et les politiques de commercialisation d'un certain nombre d'opérateurs font que si la personne ne veut pas donner le code d'accès on ne peut plus rentrer dans les téléphones »*, a souligné M. Molins. La totalité des données deviennent ainsi inaccessibles à quiconque ne possède pas le code de déblocage.

## PLUSIEURS TÉLÉPHONES N'ONT TOUJOURS PAS ÉTÉ « CASSÉS »

Une difficulté qui rend les enquêteurs *« aveugles »* dans certains cas et les prive de moyens d'investigation, a regretté M. Molins, en citant notamment le cas de Sid Ahmed Ghlam.
L'un des téléphones de l'étudiant algérien soupçonné d'un projet d'attentat contre une église de Villejuif au printemps n'a, en effet, toujours pas été « *cassé* » par les policiers. Mais un iPhone 4S saisi dans le cadre de l'enquête sur le 13 novembre garde également, à ce jour, tous ses mystères.
Dans les jours qui ont suivi les attentats du 13 novembre, la direction centrale de la police judiciaire (DCPJ) a ainsi demandé à tous ses services de résumer les problèmes posés par les *« téléphones cryptés ».« Les téléphones de dernière génération disposent de codes verrous très compliqués à casser ou contourner »*, expliquait au *Monde* le service central de l'informatique et des traces technologiques de la police judiciaire (SCITT) en réponse à la demande de la DCPJ.

De quoi inquiéter ces experts de la police scientifique : *« Les solutions utilisées ne sont pas pérennes, dans la mesure où elles sont basées sur l'exploitation de failles logicielles, le plus souvent corrigées lors des mises à jour. »* C'est le cas de l'iPhone de l'enquête du 13 novembre.

En 2014, sur 141 téléphones analysés par le SCITT, six n'ont pu être explorés. Quant à 2015, *« huit smartphones n'ont pas pu être pénétrés dans des affaires de terrorisme ou de crime organisé »*, a détaillé M. Molins.

Concernant le cryptage, *« il n'existe à ce jour aucune solution permettant aux services techniques de déchiffrer systématiquement les données »*, assure la sous-direction de la lutte contre la cybercriminalité, également sollicitée par *Le Monde*.

## UNE ACTION JURIDIQUE POUR REMÉDIER AU PROBLÈME

Deux solutions s'offrent alors aux services d'enquête judiciaire. D'abord faire appel à la direction générale de la sécurité intérieure (DGSI). Mais le centre technique d'assistance du service de renseignement répond dans un délai moyen de trois mois, et sans garantie de succès. De toute façon, reconnaît une source à la DCPJ, *« cette possibilité semble ignorée par de nombreux services »*. Les policiers peuvent aussi, éventuellement, se tourner vers les fabricants, dont certains, comme Apple, acceptent désormais, *« dans le cadre d'une urgence vitale »*, de communiquer les données stockées dans le « cloud ». A supposer qu'une sauvegarde ait été réalisée par le mis en cause.
Autant dire que le pessimisme règne du côté des services d'enquête comme des experts de la police technique et scientifique. *« Il paraît illusoire d'attendre une solution multisupport qui permettrait un accès aux données verrouillées. Seule une action juridique pourrait permettre d'obtenir ces données par le biais d'un instrument légal… Le problème réside cependant dans le poids d'un tel outil juridique face à des opérateurs ou des industriels ayant leur siège à l'étranger »*, conclut le SCITT.

---

Réagissez à cet article

Source : *Les téléphones cryptés, casse-tête des enquêtes antiterroristes*

Par Laurent Borredon

---

# Un malware soupconné d'être à l'origine d'une coupure de courant en Ukraine


# Un malware soupçonné d'être à l'origine d'une coupure de courant en Ukraine

**Le 23 décembre, les habitants de la ville ukrainienne d'Ivano-Frankivsk ont subi une importante panne de courant. Celle-ci a été provoquée par une défaillance provenant de la centrale électrique régionale et a affecté plusieurs milliers de foyers de la région. Mais cette soudaine panne n'était pas un accident : en effet, la société chargée de l'exploitation de la centrale a précisé que celle-ci avait été causée par des « interférences » sur leurs systèmes.**

Mais pour plusieurs médias locaux, la piste d'une cyberattaque visant les infrastructures énergétiques du pays est à privilégier. La société de cybersécurité ESET a d'ailleurs publié plusieurs informations en ce sens : la société explique avoir récupéré des samples de malware ayant affecté plusieurs centrales ukrainiennes, et explique que ceux-ci ont pu être utilisés dans le cadre d'une cyberattaque à l'encontre des équipements ukrainiens.

## Des nouvelles du cyberfront


ESET se dit en mesure d'affirmer que plusieurs entreprises Ukrainiennes du secteur de l'énergie sont victimes de cyberattaques. Les attaquants ont notamment recours à une famille de malware baptisées BlackEnergy, dont les traces ont été détectées à plusieurs reprises en 2015 dans des entreprises ukrainiennes liées au secteur de l'énergie.
BlackEnergy est un malware connu, qui a déjà été repéré plusieurs fois par le passé. Celui-ci se présente sous la forme d'un malware modulaire : une fois la cible infectée, les attaquants peuvent exploiter la porte dérobée ainsi créée afin de télécharger des modules différents permettant au malware d'accomplir diverses actions sur la machine cible.
Parmi les modules identifiés de ce malware, l'un d'entre eux permet notamment de s'attaquer aux systèmes SCADA, des postes utilisés pour le contrôle et la surveillance des installations industrielles. BlackEnergy permet également le téléchargement d'un autre malware, baptisé cette fois killdisk, et dont l'objectif est la destruction de données. Un arsenal qui laisse ESET penser que ces outils ont pu être mis en œuvre dans l'attaque dont semble avoir été victime la centrale électrique d'Ivano-Franivsk.
Les services de sécurité ukrainiens accusent la Russie d'être à l'origine de l'attaque selon Reuters, mais ces derniers n'ont émis aucun commentaire venant confirmer ou infirmer cette théorie. Une enquête a été ouverte par les autorités nationales pour déterminer les circonstances exactes de cette coupure de courant.

---

Réagissez à cet article

Source : *Ukraine : un malware soupconné d'être à l'origine d'une coupure de courant*

# Les 5 dangers pour vos ordinateurs, smartphones et données en 2016


Les 5 dangers pour vos ordinateurs, smartphones et données en 2016

**Les 5 tendances qui motiveront leurs actions envers votre ordinateur, votre smartphone, vos données…**

Ecartelée entre la démocratisation de l'Internet des objets (thermostat intelligent, balance connectée…), la prise de pouvoir du stockage dans le « cloud » et l'émergence des nouveaux smartphones vedettes, la sphère des nouvelles technologies subira en 2016 les assauts des virus virulents, des arnaques en ligne, des cybercriminels.
Comme un caméléon virtuel, la cybercriminalité s'adaptera plus que jamais à l'air du temps pour exploiter les nouveaux territoires en friche.
Entre prudence et clairvoyance, voici les 5 tendances cybercriminelles qui se développeront ces 12 prochains mois, selon les experts de l'éditeur de solution de sécurité BullGuard.

**1. La montée en puissance du « ransomware »**
Impitoyable méthode d'extorsion, le « ransomware » bloque votre ordinateur, crypte vos fichiers personnels et vous réclame un paiement en ligne pour les libérer.
La menace brandie en cas de refus de payer la rançon : l'extermination de vos données (photos, vidéos, documents…).
Alors que les virus à l'ancienne et les chevaux de Troie accusent une certaine perte de vitesse, le « ransomware » est appelé à les dribbler.
Ces logiciels malveillants s'attrapent en visitant un site préalablement « hacké » (piraté) ou un obscur site volontairement malveillant, en téléchargeant des fichiers vérolés, notamment sur les plateformes d'échange de fichiers illégaux…

**2. Le smartphone, cette cible indiscrète**
Connecté à Internet 7 jours sur 7, 24 heures sur 24 dans le scénario le plus extrême, le smartphone concentre une myriade de données personnelles, des adresses email de vos contacts au numéro de votre carte de crédit.
Le téléphone est par conséquent une cible de choix pour les cybercriminels, qui rivalisent d'ingéniosité pour contourner les nouvelles barrières de sécurité régulièrement déployées par Apple pour ses iPhone et Google pour son système d'exploitation mobile Google Play.
Après avoir concentré leurs efforts sur la Chine et l'Extrême-Orient, les cybercriminels devraient viser tout particulièrement l'Europe en 2016.
Certes, nos smartphones étaient déjà menacés par le virus et les logiciels malveillants. Hélas, le niveau d'alerte devrait grimper de quelques degrés.

**3. L'Eldorado inquiétant de l'Internet des objets**
Nouvelle marotte des constructeurs, l'Internet des objets entend envahir notre quotidien pour évaluer et prédire nos besoins, mesurer notre activité, adapter l'éclairage et le chauffage de notre habitation en fonction de nos usages…
Qu'il s'agisse d'un pèse-personne connecté ou d'un thermostat intelligent, ces appareils vulnérables de par leur connexion constante à Internet récoltent au kilo les données personnelles.
Imaginons le cas d'une caméra de sécurité connectée. Elle pourrait simplement être détournée par un cybercriminel pour détecter les moments où vous quittez votre maison.
Toujours en quête d'un standard, notamment pour la sécurité, la galaxie de l'Internet des objets, tout juste née de son Big Bang historique, ne manquera pas de révéler en 2016 ses failles et ses vulnérabilités.

**4. Des nuages dans le ciel du « cloud »**
Inexorable lame de fond qui modifiera à jamais le monde du stockage, le « cloud » éparpille données et fichiers dans un nuage de serveurs (ordinateurs) répartis dans d'immenses « data center » aux quatre coins du monde.
Ces « fermes » informatiques dédiées au stockage et au traitement des données présentent un double intérêt pour les cybercriminels.
Leur puissance peut être détournée à d'autres fins, tandis que les données stockées constituent un sérieux trésor de guerre au cœur duquel il est tentant de piocher.
Objet de toutes les attentions des esprits mal intentionnés, la vulnérabilité du « cloud » risque d'être régulièrement soulignée ces prochains mois.

**5. Les gangs sous les projecteurs**
Les cybercriminels se structurent en gangs d'une efficacité redoutable, souligne BullGuard.
« Ils passent des semaines, voire des mois, à effectuer des missions de reconnaissance avant d'attaquer des organisations », témoignent les experts de l'éditeur. « Ces entreprises ont été conçues dès le départ pour se spécialiser dans les crimes informatiques et ont des hiérarchies cloisonnées qui incorporent des programmeurs spécialisés dans le piratage, de vendeurs de données et des gestionnaires, tous supervisés par un cadre supérieur. Ces équipes de cybercriminels occuperont le devant de la scène en 2016. »

---

Réagissez à cet article

Source : *Virus, arnaques en ligne, cybercriminalité : les 5 dangers de l'année 2016 – L'Avenir Mobile*

# The Current State of Ransomware


## The Current State of Ransomware

**In the past year or two, one of our most popular technical topics, for all the wrong reasons, has been ransomware.**
Ransomware, as we're sure you know, is the punch-in-the-face malware that scrambles your files, sends the only copy of the decryption key to the crooks, and then offers to sell the key back to you.
Even Linux has ransomware these days, although fortunately we've only seen one serious attempt at Linux-based extortion so far, presuambly because cybercriminals haven't yet figured out how to make money in that part of the IT ecosystem.
Let's hope it stays that way for Linux sysadmins, because the crooks are still attacking Windows users heavily, and are still raking in lots of ill-gotten gains.

**THE CRYPTOLOCKER YEARS**
Two years ago, one strain of ransomware known as CryptoLocker dominated the demanding-money-with-menaces malware scene.
The US Department of Justice (DoJ) suggested that the crew behind CryptoLocker raked in $27,000,000 in September and October 2013 alone, in the first two months that the malware was widely reported.
And a 2014 survey by the University of Kent in England estimated that 1 in 30 British computer users had been hit by CryptoLocker, and that 40% of those coughed up, paying hundreds of dollars each in blackmail money to recover their data.
But in mid-2014, the DoJ co-ordinated a multi-country takedown of a notorious botnet called Gameover Zeus that targeted victims while they were doing online banking.
And, would you believe it: while the cops were raiding the Gameover servers, they came across the CryptoLocker infrastructure as well, and took down those servers at the same time, pulling off a neat double play.
CryptoLocker doesn't start its data scrambling until after it has called home for an encryption key, so killing its servers pretty much neutralised the warhead of the malware: it would get right to the very brink of detonation and then freeze, waiting for data that never came.
But any celebration about the damage done to the ransomware scene as a whole was short-lived.

**RANSOMWARE REDUX**
Cybercrime, if you will tolerate a clumsy metaphor, abhors a vacuum, and new ransomware soon appeared to fill the multi-million-dollar void left by the demise of CryptoLocker.
CryptoWall, and its close derivative CryptoDefense, were early pretenders to CryptoLocker's throne, but many others have appeared, too.
Threats like TorrentLocker, CTB-Locker and TeslaCrypt are big names these days, joined by other intriguing threats such as VirLock, ThreatFinder (an ironic name, considering that it is itself the threat) and CrypVault.

**WHAT TO DO?**
When it comes to malware of this sort, the dictum "know your enemy" is worth remembering.
With this in mind, James Wyke and Anand Ajjan, who are Senior Threat Researchers in SophosLabs, have recently published a thorough and well-written paper entitled The Current State of Ransomware.
This paper is a highly-recommended read – and it's a free download, no registration required.
https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-current-state-of-ransomware.pdf?la=en

You'll learn about the history of ransomware, the latest threats, how they work, and what you can do to defend yourself.
Great stuff from SophosLabs!

---

Réagissez à cet article

Source : *The Current State of Ransomware – a new paper from SophosLabs |*

# Quelles sont les modalités de blocage des sites Internet ?

| | |
|---|---|
|  | Quelles sont les modalités de #blocage des sites Internet ? |

**M. Lionel Tardy interroge M. le ministre de l'intérieur sur le décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographiques.**
Ce décret précise les modalités d'applications de l'article 6-1 de la loi pour la confiance dans l'économie numérique (LCEN). En complément, il souhaite savoir si, une fois la procédure appliquée, l'OCLCTIC sera également destinataire de données statistiques relatives aux tentatives de connexions aux sites bloqués, et le cas échéant, les modalités de ce recueil.

**Texte de la réponse**
La loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme a doté la France de nouveaux moyens face à la menace constante et croissante à laquelle elle est confrontée. Elle permet, notamment, de mieux combattre la propagande terroriste sur internet. Ses textes réglementaires d'application ont été rapidement publiés et toutes ses dispositions sont donc aujourd'hui applicables. Il en est ainsi des dispositions visant, suivant un dispositif gradué et équilibré garantissant le respect des libertés publiques, à renforcer les capacités de blocage des sites internet faisant l'apologie du terrorisme ou y provoquant. Le décret d'application a été publié dès le 5 février 2015 (décret no 2015-125 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique). S'agissant du nombre de connexions à un site dont l'accès est bloqué, il fait l'objet d'une comptabilisation assurée par la sous-direction de lutte contre la cybercriminalité de la direction centrale de la police judiciaire. Cette comptabilisation s'inscrit dans une démarche d'évaluation du dispositif mais vise aussi à mieux appréhender l'évolution du comportement des internautes. Lorsqu'un internaute tente de se connecter à un site dont l'accès est bloqué, il est immédiatement renvoyé sur une page d'information du ministère de l'intérieur, lui expliquant la nature du blocage et l'informant sur les voies de recours. L'adresse IP est enregistrée. Les adresses IP ainsi collectées ne sont pas exploitées mais permettent une comptabilisation précise du nombre de connexions à chacune des pages bloquées. Les premiers chiffres enregistrés depuis la mise en place du dispositif font apparaître plus de 30 000 connexions par semaine concernant les sites de pédo-pornographie, et 250 connexions en moyenne par semaine concernant les sites à caractère terroriste. Différents éléments peuvent expliquer cet écart. Dans la liste des sites dont l'accès est bloqué, ceux concernant la pédo-pornographie sont plus nombreux que ceux provoquant à des actes terroristes ou en faisant l'apologie (rapport de 3 pour 1). Par ailleurs, les connexions aux sites pédo-pornographiques ne sont pas toujours volontaires (liens publicitaires sur sites pornographiques légaux, « pourriels », etc.). Au-delà de ces dispositions nationales, le ministère de l'intérieur a engagé plusieurs actions à l'échelle européenne et internationale. En témoignent, notamment, les récentes rencontres du ministre de l'intérieur avec les grands acteurs américains de l'internet pour les amener à davantage participer à la régulation des contenus appelant à la commission d'actes terroristes ou en faisant l'apologie. Ces travaux ont notamment permis de décider la création d'une plate-forme de bonnes pratiques dans la lutte contre la propagande terroriste sur internet.

---

Réagissez à cet article

Source : *Question n°74166 – Assemblée nationale*