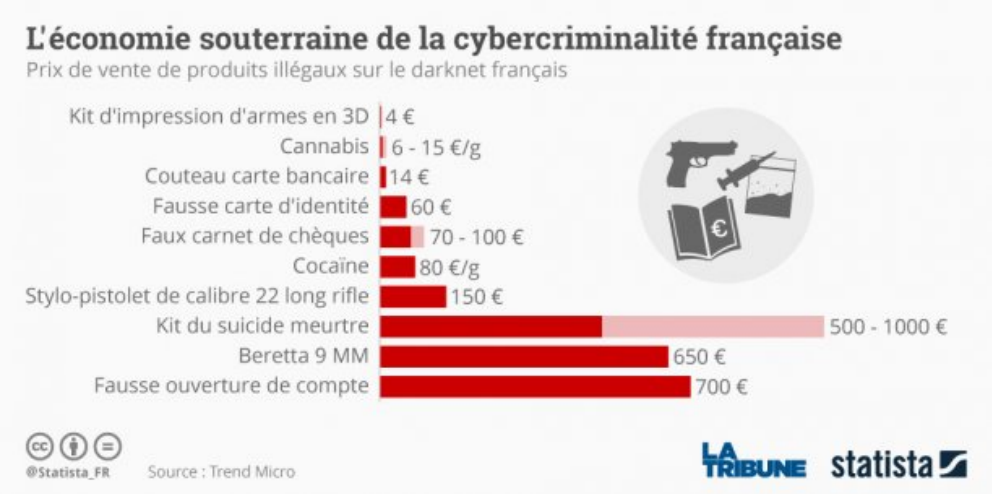
Qui sont les escrocs du darknet français ?



Qui sont les escrocs du darknet français ?

Pour la première fois, une étude, réalisée par la société de cybersécurité Trend Micro, s'est penchée sur l'organisation de la sphère cybercriminelle française. D'après ses estimations, 40.000 escrocs réalisent un chiffre d'affaires compris entre 5 et 10 millions d'euros par mois.

À quoi ressemble l'économie souterraine de la cybercriminalité française ? Combien de hackers malveillants y prospèrent ? Comment s'organisent-ils, que vendent-ils et combien gagnent-ils ? Pour la première fois en France, une étude, réalisée par l'entreprise de cybersécurité Trend Micro et publiée ce mercredi, donne des réponses. Pendant un an, ses équipes de R et D ont scruté les marchés souterrains nationaux et compris ses spécificités.
Le panorama dressé, plutôt inquiétant, révèle les dessous du « web underground » français. Un écosystème criminel qui prospère dans le *darknet* (l'internet caché), mais qui apparaît très bien organisé, en pleine professionnalisation et… en pleine croissance.

40.000 cybercriminels dans une centaine de places de marché

Selon les estimations de l'auteur de l'étude, qui souhaite rester anonyme, le cybercrime français se compose de 40.000 individus. Un chiffre « relativement faible » par rapport aux marchés plus importants comme la Russie ou les États unis, mais comparable à celui de l'Allemagne. Ce chiffre a été obtenu en compilant et en pondérant le nombre de membres de la centaine de « marketplaces » du *darknet*, c'est-à-dire les forums de discussions qui sont indispensables aux hackers pour organiser leurs fraudes.
Quel est le profil de ces cybercriminels ? Bien évidemment, tout le monde utilise un ou plusieurs pseudo, des plus loufoques aux plus lyriques. Mais les connaisseurs de ce milieu estiment qu'il s'agit surtout d'hommes jeunes, entre 20 et 30 ans. Au regard de leurs compétences techniques, certains sont « *certainement des développeurs professionnels*« . On assiste aussi au retour en force des anciens « spammers nigérians », les escrocs qui envoyaient des courriels pour demander de l'aide dans les années 1990 et 2000, et qui se reconvertissent désormais dans les virus informatiques.
Relatif soulagement : la plupart des 40.000 cybercriminels français ne vivent pas exclusivement de cette activité. Seule une petite centaine d'entre eux seraient « de vrais pros ». Les autres sont plutôt à la recherche d'un complément de revenus. Mais cela n'empêche pas cet écosystème de prospérer. D'après les données de la Gendarmerie nationale et de la Police nationale, la cybercriminalité française générerait entre 5 et 10 millions d'euros de chiffre d'affaires tous les mois.

Armes, drogues, données bancaires

Les places de marché, qui attirent au moins plusieurs milliers, voire une dizaine de milliers d'utilisateurs chacune (la plupart du temps, les hackers sont membres de plusieurs forums) sont très bien structurées, avec des sous-sections clairement identifiées en fonction des « besoins » : armes, logiciels malveillants, drogues…
Comment s'organise ce commerce ? « *Généralement, il existe trois canaux de vente de biens et de services illégaux au sein de l'underground français* », décrypte l'étude. Certains fraudeurs font la promotion de leurs produits directement sur les places de marchés. D'autres, plus paranoïaques, guettent les messages et contactent eux-mêmes leurs clients. Enfin, il existe aussi des « autoshops », c'est-à-dire de véritables boutiques gérées par les vendeurs eux-mêmes, dont beaucoup sont accessibles depuis les forums. C'est même la grande spécialité française.
Les vendeurs proposent un catalogue impressionnant de produits illégaux, à des prix très compétitifs. On y trouve des armes discrètes (poings américains, couteaux de petits formats, stylo-pistolets de calibre 22 long rifle), vendues entre 10 et 150 euros. Mais aussi des armes lourdes, vendues entre 650 et 1.800 euros, ainsi que des kits d'impression d'armes en 3D, que l'on peut acquérir pour une poignée d'euros.
Au rayon des stupéfiants, le cannabis se vend entre 6 et 15 euros le gramme, mais on trouve aussi de la cocaïne, de l'héroïne, de la MDMA, du LSD et autres champignons. »*Les dealers ne vendent qu'en France pour ne pas se faire détecter lors des transactions transfrontalières* », note l'étude. Les autoshops proposent également des fichiers comportant des bases de données personnelles (comme des numéros de carte bancaire) pour environ 400 euros…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- 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.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Cybercriminalité : qui sont les escrocs du darknet français ?

Alerte : Le ransomware Locky passe en mode autopilote

	Alerte : Le ransomware Locky passe en mode autopilote

---

Une nouvelle variante de Locky ajoute un mode autopilote qui proscrit les connexions aux serveurs de commandes et contrôles. Un mode toujours plus discret.
Il n'y a pas que les voitures autonomes qui se pilotent toutes seules (parfois avec des conséquences dramatiques). Les malwares aussi (avec des conséquences moins dramatiques humainement mais qui peuvent s'avérer aussi ennuyeuses qu'onéreuses). Locky, l'un des ransomwares les plus actif et tristement célèbre, connaît une nouvelle évolution. Il vient de passer en mode d'auto-pilotage. Autrement dit, l'agent malveillant n'a plus besoin de se connecter à un serveur distant de contrôle et commandes (C&C) pour engager le chiffrement des fichiers victimes de son attaque. C'est du moins ce qu'ont découvert les chercheurs en sécurité de l'éditeur Avira.

Locky en mode furtif
L'autopilotage permet désormais à Locky d'opérer en mode furtif. « Avec cette étape, [les attaquants] n'ont plus à jouer au chat et à la souris avec la mise en place incessante de nouveaux serveurs avant qu'ils ne soient blacklistés ou fermés », commente Moritz Kroll, spécialiste des logiciels malveillants au Protection Labs d'Avira. Il rappelle en effet que, précédemment, la configuration de Locky comprenait des URL pointant vers des serveurs de C&C ainsi qu'un algorithme de génération de domaines pour créer des liens supplémentaires vers des serveurs de commande et contrôle.
En se libérant de cette dépendance, le mode Autopilote du malware permet à ses auteurs (ou utilisateurs) d'économiser des coûts d'infrastructure et optimiser ainsi la rentabilité de leurs opérations. « Les cybercriminels affinent le mode d'infection 'hors-ligne', ajoute le chercheur d'Avira. En réduisant au minimum les activités en ligne de leur code, ils n'ont pas à payer pour autant de serveurs et de domaines supplémentaires. » Et si ce mode de fonctionnement déconnecté ne leur permet plus de remonter les statistique des infections en cours, il présente l'avantage de se montrer plus discret aux yeux des responsables du réseau. « Auparavant, les administrateurs systèmes pouvaient bloquer les connexions aux serveurs C&C et se prémunir des opérations de chiffrement de Locky. Ces jours sont désormais révolus, prévient Moritz Kroll. Locky a réduit les chances des victimes potentielles d'éviter une catastrophe de chiffrement. »…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**.
Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- 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.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Ransomware : Locky active le mode pilotage automatique

---

8 failles critiques dans Android corrigées

	8 failles critiques dans Android corrigées

---

Alors que Google s'était déjà illustré au mois de juin en apportant 28 corrections au système d'exploitation mobile Android, la firme de Mountain View a livré il y a quelques heures une nouvelle salve de correctifs. 8 failles critiques ont d'ailleurs été patchées !

Encore des corrections en masse pour Android

Souvent décrié en raison du nombre de failles qui affectent son célèbre système d'exploitation mobile, Google a une nouvelle fois livré un nombre (trop) important de patchs correctifs et le problème, c'est que plusieurs vulnérabilités corrigées sont estimées comme « critiques ».

Eh oui, aussi surprenant que cela puisse paraître, la société implantée à Mountain View vient bel et bien d'apporter 57 correctifs dont 8 ont servi à patcher des failles pouvant s'avérer être une vraie menace pour les terminaux.

Trois sets de correctifs disponibles

Le premier set, disponible depuis le 1er septembre 2016, permet de combler 25 failles Android. Deux d'entre elles étaient critiques. L'une permettait d'exécuter du code distant via une attaque de type « dépassement de mémoire » au niveau du package libutils d'Android. L'autre donnait la possibilité d'exécuter du code distant dans les composants Mediaserver d'Android.

Le deuxième set, mis en ligne le 5 septembre 2016, propose quant à lui de corriger 30 failles exposant largement l'utilisateur. Les plus critiques permettent d'obtenir des privilèges système, d'accéder à un noyau de sous-système réseau, de netfilter ou encore de driver USB…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- 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.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Encore 8 failles critiques patchées dans Android

L’Agence mondiale anti-dopage victime de piratage

L’Agence mondiale anti-dopage victime de piratage

L'Agence mondiale anti-dopage (AMA ou WADA en anglais) a été victime d'un piratage. Un groupe de hackers a pu subtiliser les dossiers médicaux de quatre athlètes américaines et dévoiler des informations confidentielles. Surprise : les pirates sont russes !

Les Russes l'auraient-ils mauvaise suite à la disqualification de la quasi-totalité de leurs athlètes lors des Jeux Olympiques de Rio ? Ce vaste « nettoyage » opéré par les fédérations sportives internationales faisait suite au scandale sur le dopage d'Etat généralisé en Russie. Toujours est-il que le groupe russe Tsar Team (APT28), Fancy Bear pour les intimes, a piraté une base de données de l'AMA.
La date exacte de l'attaque n'est pas connue. Les hackers ont vraisemblablement obtenu l'accès aux serveurs de l'Agence en obtenant par phishing des mots de passe ADAMS (pour Anti-Doping Administration and Management System, le SI de l'AMA), via un compte du Comité International Olympique créé à l'occasion des JO de Rio. Ils ont ainsi pu dérober les données relatives à quatre athlètes américaines, notamment leurs dossiers médicaux détaillés.

Simone Biles, quadruple championne olympique en athlétisme

Sur les réseaux sociaux, Fancy Bear a divulgué une partie de ces informations, pointant du doigt des « *analyses anormales* » dans les dossiers des joueuses de tennis Venus et Serena Williams, de la basketteuse Elena Delle Donne et de la gymnaste Simone Biles. L'AMA a pris la défense des athlètes mises en cause, expliquant qu'elles bénéficient d'exemptions thérapeutiques. Dans le cas de Simone Biles, par exemple, il s'agit d'un traitement pour trouble du déficit de l'attention, dont il avait déjà été question lors des JO. Mais les hackers promettent bien d'autres révélations.

« Miner le système anti-dopage mondial ».

Le CIO a condamné cette attaque, « *destinée à salir la réputation d'athlètes propres* ». L'AMA elle aussi condamne, et y voit une tentative de « *miner le système anti-dopage mondial* »…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- 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.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Des hackers russes derrière le piratage de l’Agence mondiale anti-dopage

---

Comment préparer les enfants aux Réseaux Sociaux ?

Comment préparer les enfants aux Réseaux Sociaux ?

Dangers de l'Internet au-delà de logiciels malveillants, ou l'enlèvement des données par des ransomware. Sur le Net, le respect de la vie privée est mis à mal par les réseaux sociaux, les moteurs de recherche et la publicité. Dans le cas des mineurs, il y a des risques plus inquiétants, dont ils ne sont pas pleinement conscients, mais leurs parents, les enseignants et la société doivent assurer leur sécurité. Une étude récente, appelé Kids Connected, et menée par la firme de sécurité Kaspersky Lab avec iconKids et jeunesse, révèle des faits troublants sur la façon dont les enfants se comportent en ligne. Comportements qui peuvent conduire à provoquer plus de crainte.

Ce rapport montre que **les enfants âgés de 8 à 16 ans sont accros aux réseaux sociaux**. En outre, l'activité peut les mettre en danger, eux et leurs **familles**. 35% des enfants disent qu'ils ne veulent pas être sans réseaux sociaux, et sont désireux de rejoindre des groupes en leur sein, ils sont en mesure de partager beaucoup d'informations personnelles. **Le problème** est qu'ils le font sans avoir conscience que les données qu'ils partagent sont vues par de nombreux utilisateurs et peuvent être utilisées par des personnes potentiellement dangereuses.

Trop d'informations personnelles

Mais **qu'est-ce que les mineurs partagent le plus** ? La plupart des enfants, 66%, **montrent l'école** où ils étudient, 54% **des lieux qu'ils visitent**, et 22% partagent même **la gestion de leurs maisons**. Mais, 33% des enfants donnent également des **informations sur les effets de leur famille et de leurs parents**, sur leur travail (36%) ou sur **ce que leurs parents facturent** (23% des enfants).
Mais, outre le partage des données réelles, **les mineurs sont également prêts à mentir sur le réseau**, et ils le font surtout **si ça peut leur ouvrir des portes**. Un tiers des enfants est prêt à mentir au sujet de l'âge. 17% des enfants font semblant d'être plus âgés, et de modifient leur âge en fonction du web ou le service qu'ils veulent utiliser, étant donné que beaucoup d'entre eux ont des restrictions (très facile à sauter) d'âge.
Avec ces données, **les cybercriminels disposent d'informations suffisantes pour être utilisés à des fins malveillantes**. Parmi les activités criminelles qu'ils pourraient commettre, ils trouvent l'emplacement physique des mineurs. **Tous les enfants doivent apprendre à un âge précoce ce qu'ils devraient partager en ligne**, ou non. Et connaître les paramètres des réseaux sociaux de la vie privée, de sorte que seuls leurs amis peuvent voir leurs publications et leurs données.

Comprendre quelles sont vos données et la façon de les protéger

Tous les enfants et leurs parents doivent comprendre ce que sont les données personnelles, et **la façon dont on peut les protéger**. "Ceci est comparable aujourd'hui à lire et à écrire», dit Janice Richardson, consultant senior chez European Schoolnet, qui explique que **«les enfants ont besoin d'apprendre à un âge précoce que la vie privée est votre bien le plus précieux, et un droit fondamental ».**
Comme des **conseils de base** qui sont donnés par Kaspersky Lab afin d'éviter autant que possible les risques:
• Une bonne **communication est essentielle**. Il faut parler aux enfants au sujet de leurs expériences et préoccupations.
• **Réalisez les premières étapes dans les réseaux sociaux avec eux** pour créer le profil, activez les options de confidentialité, publiez votre premier poste …
• Les réseaux sociaux ont des **restrictions d'âge**. La plupart sont fixée à 13 ans. À cet âge, il est commode d'en profiter pour leur parler et leur expliquer leurs droits, les responsabilités et les préparer à l'entrée dans le monde numérique.
• Cela peut **devenir un jeu**, quelque chose que vous faites en famille: par exemple, l'impression de leur profil, accroché au mur, leurs postes … Ils pourront visualiser le public à qui est destiné chaque contenu.
• **Établir des règles** pour leur utilisation.
• **Encourager les enfants à communiquer avec vous**, ils vous apprendront de nouvelles applications récemment installées, les services qu'ils utilisent … Si cela devient une habitude depuis le début, il sera plus facile de partager des informations et de leur **parler de la vie privée et de sécurité**.

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- 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.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : La situation préoccupante des enfants dans le réseau: mentir pour accéder aux réseaux sociaux et y donner trop d’informations

---

Trend Micro ausculte la cybercriminalité underground en France

	A quoi ressemble de DarkNet ?

L'éditeur de sécurité a dressé un état des lieux de l'underground de la cybercriminalité en France. Méfiance, bitcoins et forte orientation vers les falsifications des documents sont les maîtres mots.
Un chercheur de Trend Micro s'est livré à un exercice délicat : plonger dans l'univers de la cybercriminalité souterraine en France. Connu sous le vocable « underground », cette partie du web accueille des places de marchés, des forums où s'achètent contre monnaie virtuelle des armes, de la drogue, des faux documents, mais aussi des malwares.
Dans son étude, l'éditeur japonais précise que le tréfonds du web français reste relativement modeste par rapport à d'autres pays comme la Chine ou la Russie. Néanmoins, il recense 40 000 cybercriminels sur l'underground hexagonal ayant des compétences hétérogènes (expert à novice). Ce foyer génère entre 5 à 10 millions d'euros par mois.

Une prudence de sioux
Un des leitmotiv des cybercriminels français est la prudence. Pour approcher ce monde souterrain, il faut montrer patte blanche. L'objectif est d'éviter de se faire coincer par les forces de l'ordre. Le climat de méfiance règne donc allant jusqu'à la délation (signalement des actes malhonnêtes et frauduleux) et jusqu'à l'affrontement (les places de marché se piratent mutuellement pour se piquer des clients).
L'acceptation sur les forums fait par cooptation, par évaluation de la réputation. Mais ce qui distingue le Dark Net Français, c'est le recours à des tiers de confiance (escrow en anglais). Ils jouent un rôle d'intermédiaire dans la transaction entre les deux parties pour s'assurer que chacun récupère son dû. Ces intermédiaires prennent une commission (entre 5 et 7%) sur la transaction. Certaines places de marché ont même créé leurs propres plateformes de tiers de confiance (mais faut-il encore avoir confiance ?).
La disparition des forums est aussi un grand classique, comme le précise le chercheur de Trend Micro. « Un des forums les plus en vue du French Dark Net qui recensait 40 000 utilisateurs avec la possibilité de gérer leurs transactions a fermé du jour au lendemain et les administrateurs se sont enfuis avec la caisse. Le préjudice est estimé à 180 000 euros. » Et d'ajouter que les mêmes administrateurs ont créé une nouvelle structure dans les jours suivant. Rien ne se perd, tout se crée.

Chiffrement et bitcoin de rigueur
Parmi les autres enseignements, l'underground français n'échappe pas à la vague du chiffrement des communications. Logique, avec un degré de méfiance qui frise la paranoïa, les conversations sont chiffrées et plutôt fortement, assure Trend Micro. « On est principalement sur du PGP. » De même, l'usage de Tor s'est banalisé. Pour trouver les forums ou les places de marché, il est quasiment impossible de les repérer sur le web normal. Les sites se terminent par .onion indiquant son appartenance au réseau anonymisé Tor.
Le Bitcoin et les cartes prépayées sont les moyens de paiement préférés sur l'underground français. La crypto-monnaie est traditionnellement utilisée dans ce genre de secteur. Mais la carte prépayée PCS est une spécificité française. « Elles sont devenues si populaires que certains cybercriminels vendent ce type de cartes avec de faux papiers d'identité et des fausses informations personnelles comme adresse physique, e-mail et carte SIM. L'objectif est de déverrouiller le plafond de paiement pour atteindre jusqu'à 3000 euros. L'opération coûte à peu près 60 euros », souligne Trend Micro.

Le royaume des faux documents officiels et Pass PTT
Héritage du système jacobin et du régime napoléonien, la France est la partie des papiers administratifs. On ne s'étonnera donc pas que les propositions commerciales sur le Dark Net hexagonal concernent la fraude aux documents administratifs. Fausse carte d'identité, carte grise (500 euros), carte PMR (mobilité réduite pour 40 euros), justificatif de domicile (utile pour certaines démarches), vente de points pour le permis de conduire, ouverture d'un compte bancaire (700 euros).
Autre élément typiquement français, le pass PTT. Il s'agit d'une clé dont dispose les livreurs pour ouvrir l'ensemble des boîtes aux lettres d'un immeuble. Les personnes peuvent ainsi chercher des plis contenant de l'argent, des chéquiers ou des clés de maison. Ces pass PTT sont disponibles sur les forums underground à des tarifs abordables. Un vendeur proposait 25 clés pour 220 euros, un autre vendait à l'unité au tarif de 15 euros et un troisième livrait un fichier d'impression 3D de la dite clé, rapporte l'éditeur de sécurité…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- 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.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

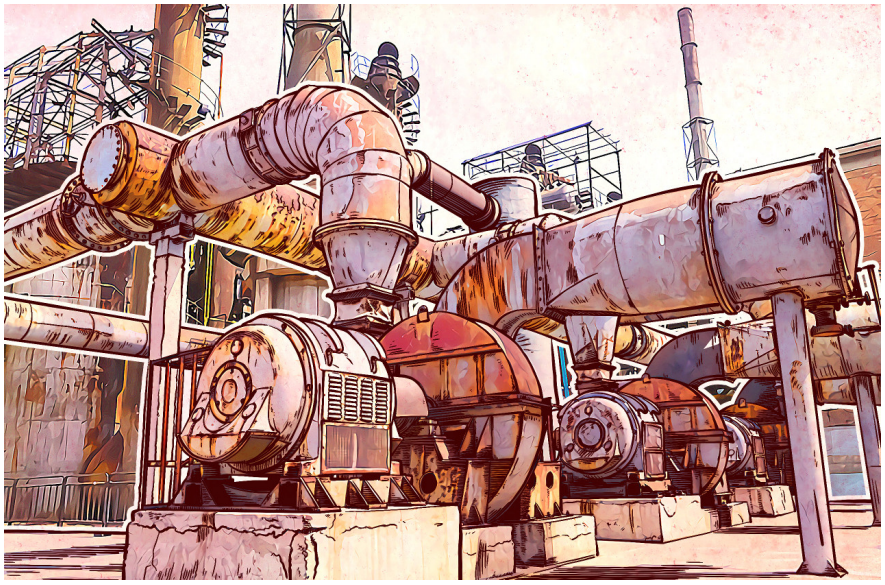
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Trend Micro ausculte la cybercriminalité underground en France

---

Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie

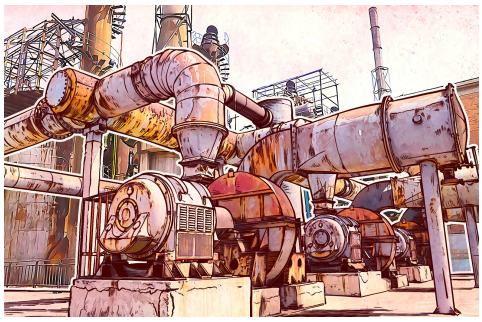


Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie

---

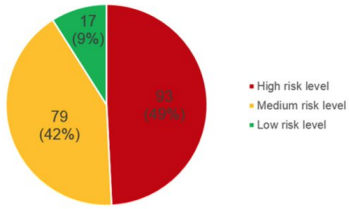
On ne cesse de vous le répéter, il est très important de rester au courant des dernières actualités concernant la cybersécurité et ses menaces. Mieux vaut prévenir que guérir.

Cependant, même ceux qui connaissent tout en matière de cybersécurité, qui utilisent des mots de passe fiables et qui les changent régulièrement, qui reconnaissent des messages d'hameçonnage au premier coup d'œil et qui protègent leurs dispositifs avec une excellente solution de sécurité, même ceux qui font *tout*, ne sont pas totalement à l'abri. Tout simplement parce que nous vivons en société.



Le problème est que nous avons le contrôle sur nos objets personnels, mais pas sur celui des équipements industriels, qui est loin de notre portée.

Vous avez dit cybersécurité ?
Nos experts en cybersécurité ont mené une étude afin de découvrir où nous en sommes concernant la sécurité des systèmes de contrôle industriel.
Shodan, le moteur de recherche pour les dispositifs connectés, nous a montré que 188 019 systèmes industriels dans 170 pays sont accessibles sur Internet. La majorité d'entre eux sont localisés aux Etats-Unis (30,5%) et en Europe, essentiellement en Allemagne (13,9%), Espagne (5,9%) et en France (5,6%).



ICS vulnerabilities in 2015 by risk level (CVSS v.2 and CVSS v.3)

92% (172 982) des systèmes de contrôle industriel (SCI) détectés sont vulnérables. Lamentablement, 87% ont un niveau de risque moyen de bugs et 7% connaissent des problèmes critiques.
Ces cinq dernières années, les experts ont méticuleusement examiné de tels systèmes et y ont découvert de nombreuses failles de sécurité. Durant ce laps de temps, le nombre de vulnérabilités dans les composants SCI a multiplié par dix.
Parmi les systèmes que nos experts ont analysés, 91,6% ont utilisé des protocoles non sécurisés, en donnant l'opportunité aux cybercriminels d'intercepter ou de modifier les données utilisant des attaques de l'homme du milieu.
Egalement, 7,2% (environ 13 700) des systèmes appartiennent à de grandes compagnies aéronautiques, des transports et de l'énergie, pétrolières et gazières, métallurgiques, de l'industrie alimentaire, de la construction et autres secteurs primordiaux.

En d'autres termes, des hackers qualifiés peuvent influencer n'importe quel secteur économique. Leurs victimes (les entreprises piratées) porteraient préjudice à des milliers ou millions de personnes en leur fournissant de l'eau contaminée ou de la nourriture immangeable, ou en leur coupant le chauffage en plein hiver.

Qu'est-ce que cela implique pour nous tous ?

…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- 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.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie. | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.

Quand les pirates s’attaquent à l’éducation

	Quand les pirates s’attaquent à l’éducation

---

Le milieu scolaire n'est pas épargné par les hackers, certains étudiants piratent les examens, les notes ou leurs professeurs, tirant profit d'outils prêts à l'emploi mais aussi d'un manque de moyens et de sensibilisation des principaux concernés.

De nombreux collèges, écoles ou lycées sont les cibles de cyber-attaques perpétrées par des étudiants. Des offensives qui : *«sont réalisées par des digital natives, des jeunes à l'aise avec l'informatique qui sont nés avec un ordinateur entre les mains»*, explique Jean-Charles Labbat, directeur général France, Belgique, Luxembourg et Afrique francophone chez Radware, société spécialisée en sécurité informatique.

Des attaques basiques

Trois secteurs sont principalement visés par ces hacks : les examens, les notes, puis les systèmes informatiques des institutions ou des professeurs. Et les méthodes utilisées ne sont pas des plus sophistiquées.
Un étudiant pas suffisamment préparé pour passer un examen (comme les QCM en ligne dans certains pays) peut essayer de bloquer le site. Pour ce faire, il utilise le déni de service, il se connecte à ce serveur et se rend au point de connexion pour y envoyer une surcharge d'informations et boucher l'accès à l'application. Un hack très simple puisque, comme l'explique Jean-Charles Labbat, *« des outils sont disponibles sur internet comme Slowloris, ou il suffit de rentrer l'adresse du serveur pour le faire tomber ».*
Pour les systèmes de notation, rien de bien compliqué non plus. Les notes sont rangées dans une base de données et pour consulter ses résultats il faut se connecter avec ses identifiants. Le pirate va recourir à une injection SQL pour rentrer sans mot de passe, accéder directement à la base de données et modifier les informations renseignées. En novembre 2014, un élève du Tarn avait augmenté sa moyenne la faisant passer de 8,76 à 10,62.
Les enseignants sont également ciblés, via l'envoi de spams par exemple. *« Les enseignants recourent de plus en plus à l'outil informatique pour leurs cours. Un étudiant malveillant peut très bien s'il le souhaite accéder à un ordinateur mal protégé, spammer son professeur mais aussi ses contacts ou affecter tout le réseau de l'école* »...[lire la suite]

Denis JACOPINI est **Expert Informatique assermenté et formateur** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-en-cybercriminalite-et-en-protection-des-donnees-personnelles

---

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- 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.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Quand les pirates s’attaquent à l’éducation > Mag-Securs

Est-ce qu’un lien vers un contenu illégal est lui aussi illégal ?

Est-ce qu’un lien vers un contenu illégal est lui aussi illégal ?

Le fait de publier un lien renvoyant vers un contenu illicite est lui-même constitutif de contrefaçon ? À cette éminente question, la Cour de justice de l'Union européenne vient de répondre que non, sous deux importantes réserves : que le lien litigieux ait été diffusé sans but lucratif et que son auteur n'ait pas eu connaissance de son illicéité.

C'est suite à une saisine de la Cour de cassation des Pays-Bas que la justice européenne a rendu son arrêt de ce jour. Au cœur de ce dossier, un vrai jeu du chat et de la souris. Une dizaine de photos d'une présentatrice hollandaise furent hébergées sur FileFactory, puis « linkées » sur Geenstijl.nl, important site néerlandais. Le renvoi vers ces images, destinées à être publiées dans l'édition nationale de Playboy, avait rapidement provoqué la colère de la revue de charme. Sauf que même après avoir réussi à obtenir leur retrait de FileFactory, de nouveaux liens furent établis par Geenstijl.nl, cette fois via ImageShack.us notamment…
D'où la question : publier des liens vers ces images signalées comme manifestement illicites constituait-il un nouvel « acte de communication » d'une œuvre au public au sens de la directive européenne relative au droit d'auteur – dès lors soumis à l'autorisation obligatoire (et préalable) des ayants droit ? Pour la CJUE, la réponse est oui…[lire la suite]
L'arrêt de la CJUE (PDF)

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- 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.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : La CJUE juge qu'un lien

vers un contenu illégal peut être illégal

Une garantie d’un million de dollars contre les ransomwares

	Une garantie d’un million de dollars contre les ransomwares

---

Un éditeur de logiciels de cybersécurité propose de reverser jusqu'à un million de dollars à ses clients qui seraient, malgré ses protections, victimes d'un virus informatique.

Ce n'est pas une incitation à payer les rançonneurs informatiques. Hier, l'éditeur de logiciels de cybersécurité SentinelOne a annoncé proposer à ses clients professionnels une garanti d'un montant maximum d'un million de dollars contre toute menace qui percerait ses défenses. Notamment les ransomwares, ses programmes malveillants qui coupent l'accès aux données stockées dans les ordinateurs touchés et invitent à payer pour les récupérer. La police conseille de ne jamais céder à ce chantage.
SentinelOne compte sur sa technologie de machine learning pour protéger ses clients. En cas de manquement à ses devoirs, l'éditeur dédommagerait les entreprises à hauteur de 1.000 dollars par postes de travail et dans la limite d'un million de dollars. « *Avec cette assurance financière, nous devenons vraiment responsables de la sécurité de nos clients*, souligne Scott Gainey, le patron du marketing de SentinelOne,*jusqu'ici, les entreprises victimes qui voulaient se retourner contre leurs éditeurs d'anti-virus ne pouvaient pas, c'est injuste*. » D'après lui, cette garantie est une première au monde…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- 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.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Une garantie d'un million de dollars contre les ransomwares, Cybersécurité — Les Echos Business