# Assange a tenté de prévenir Clinton d’une cyberattaque imminente

| | |
|---|---|
| | Assange a tenté de prévenir Clinton d’une cyberattaque imminente |

**Dans un nouveau documentaire sur Julian Assange, sorti ce samedi, la réalisatrice évoque un épisode où le fondateur de WikiLeaks essayait, en vain, d'avertir Hillary Clinton de cyberattaques contre le Département d'État.**

Le fondateur de Wikileaks Julian Assange aurait téléphoné au Département d'État américain pour avertir la secrétaire d'État Hillary Clinton d'une cyberattaque imminente contre les réseaux électroniques de la structure. La bande-annonce du documentaire «Risk», réalisé par Laura Poitras, en parle.

Le film, a été diffusé par la chaîne Showtime samedi 22/07/2017, et débute par un coup de fil d'Assange au Département d'État. Le lanceur d'alerte tente de parler personnellement à Hillary Clinton pour l'avertir que des mots de passe et divers fichiers ont été diffusés à travers le monde, raconte la voix off de la réalisatrice.

[lire la suite]

---



---

Réagissez à cet article

Source : *Assange a tenté de prévenir Clinton d'une cyberattaque imminente – Sputnik France*

# L’impossibilité de détecter la source d’une cyberattaque permet de désigner les coupables

| | |
|---|---|
| | L’impossibilité de détecter la source d’une cyberattaque permet de désigner les coupables |

**Se prononçant sur les accusations infondées concernant l'ingérence russe dans la politique d'autres pays, le chef de l'état-major général russe Valeri Guerassimov a fustigé les pays occidentaux pour avoir déclenché une guerre informationnelle.**

L'impossibilité de détecter la source d'une cyberattaque permet de désigner les coupables, a déclaré le chef de l'état-major général russe Valeri Guerassimov lors d'une Conférence sur la sécurité internationale qui se déroule aujourd'hui à Moscou.
« L'Alliance a commencé à mettre au point l'application de l'article 5 du Traité de Washington (concernant la défense collective, ndlr.) dans le cas des cyberattaques sur les dispositifs matériels des systèmes étatiques et militaires des pays membres de l'Otan. Mais dans les conditions actuelles, il est presque impossible de détecter les sources réelles de ces attaques. À cet égard, il est possible de désigner les responsables sans avoir de preuve et d'agir sur eux par des moyens militaires », a déclaré le chef de l'état-major général russe.
« Les pays occidentaux intensifient la guerre informationnelle agressive déclenchée contre la Russie. Si on regarde les articles des médias européens et américains, il semble que presque tous les événements négatifs dans le monde soient orchestrés soit par les services spéciaux russes, soit par des hackers russes », a indiqué Valeri Guerassimov….[lire la suite]

---



---

Réagissez à cet article

Source : *L'impossibilité de détecter la source d'une cyberattaque permet de désigner les coupables*

---

# Que faire en priorité en cas

# d’attaque informatique

## Que faire en priorité en cas d’attaque informatique

**Quelles sont les premières mesures à prendre lorsque l’on suspecte d’avoir été la victime d’un incident de sécurité informatique ?**

A un moment ou l’autre, votre entreprise devra faire face à un incident de cybersécurité. Mais sous la pression, l’effet du stress, on fait des erreurs. Trop reporter la prise de décisions critiques peut renforcer l’impact de l’incident, mais inversement, prendre des décisions trop hâtives peut causer d’autres dommages à l’entreprise ou entraver une réponse complète.
Il existe de nombreuses façons de soupçonner qu’un incident de sécurité s’est produit, de la détection d’activités inhabituelles par le suivi proactif des systèmes critiques jusqu’aux audits, en passant par la notification externe par les forces de l’ordre ou la découverte de données compromises perdues dans la nature.
Toutefois, des indicateurs tels que la consommation inhabituelle de ressources CPU ou réseau sur un serveur peut avoir plusieurs origines différentes, dont beaucoup n’ont rien à voir avec des incidents de sécurité. Il est là essentiel d’enquêter davantage avant de tirer des conclusions.
Disposez-vous des d’indices cohérents ? Par exemple, si l’IDS détecte une attaque de force brute contre le site Web, les journaux Web le confirment-ils ? Ou, si un utilisateur signale une attaque suspectée de hameçonnage, d’autres utilisateurs ont-ils été visé ? Et quelqu’un a-t-il cliqué sur des liens ou des documents joints ?
Vous devez également réfléchir à des questions relatives à la nature de l’incident. S’agit-il d’une infection par un logiciel malveillant générique ou un piratage de système ciblé ? Y’a-t-il une attaque intentionnelle en déni de service (DoS) en cours ?…[lire la suite]

---

**Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d’expertises, d’audits, de formations et de sensibilisation dans toute la France et à l’étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d’un Correspondant Informatique et Libertés (CIL) ou d’un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l’Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d’informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Que faire en premier en cas d’attaque informatique*

# Ressources pour la collecte et la vérification d’informations à destination des journalistes

| | |
|---|---|
| | Ressources pour la collecte et la vérification d’informations à destination des journalistes |

**Votre guide pour le traitement des contenus mis en ligne par des tiers, de la découverte à la vérification**

**Présentation de Samuel Laurent, éditeur délégué du Monde, partenaire de First Draft**
L'éditeur délégué du Monde présente à First Draft ses travaux en matière de lutte contre la désinformation en ligne et ses projets…[Lire la suite]

**Lancement de CrossCheck : à l'approche des élections françaises, les rédactions s'associent pour lutter contre la désinformation**
CrossCheck réunit les compétences des secteurs des médias et des technologies pour s'assurer que fausses déclarations soient rapidement détectées et corrigées…[Lire la suite]

**Outils pour renforcer la confiance envers les journalistes**
Fort de son expérience dans le paysage journalistique américain, Josh Stearns nous présente des outils pour que journalistes et rédactions regagnent la confiance de leur audience…[Lire la suite]
**Outils et ressources** : Hearken, Engaging News Project, Coral ProjectNews Voices Engaged Newsroom Toolkit

**Guide pour la vérification visuelle des vidéos**
Il s'agit d'un guide de référence rapide pour vous aider à identifier le qui, quoi, où, quand et pourquoi des vidéos des internautes…[Lire la suite]

**Guide pour la vérification visuelle des photos**
Il s'agit d'un guide de référence rapide pour vous aider à identifier le qui, quoi, où, quand et pourquoi des photos mises en ligne par des tiers…[Lire la suite]

**Utiliser Google Earth pour vérifier des images comme un pro**
Google Earth offre bien plus que des images satellites…[Lire la suite]

**Réseaux sociaux et contenus viraux : comment les développeurs des rédactions peuvent-ils faciliter la démystification ?**
Les nouveaux projets de vérification doivent tenir compte des leçons clés tirées des procédés de « fact-checking » (vérification par les faits) ayant faits leurs preuves, tout en les adaptant aux écosystèmes des réseaux sociaux…[Lire la suite]
**Savoir où chercher : sources d'image pour la géolocalisation**
Trouver d'autres photos ou vidéos d'un lieu peut être un des meilleurs moyens de vérifier le lieu où a été capturé un contenu. Voici où chercher…[Lire la suite]
**10 façons de mieux couvrir le terrain pour les journalistes locaux**
Combiner le reportage traditionnel sur le terrain et les possibilités offertes par les services numériques modernes peut faire la différence entre un bon et un très bon journaliste…[Lire la suite]
**Respecter la source : l'importance du témoin dans la couverture de l'actualité en temps réel**
Les témoins sont des personnages clés dans de nombreux événements majeurs se produisant aux quatre coins du monde…[Lire la suite]
**Comment se protéger face aux contenus traumatisants ?**
Sam Dubberley, cofondateur de Eyewitness Media Hub, détaille certains des résultats principaux d'une étude récente portant sur les traumatismes indirects dans les rédactions…[Lire la suite]

---



---

Réagissez à cet article

Original de l’article mis en page : First Draft News FR – Votre guide pour le traitement des contenus mis en ligne par des tiers, de la découverte à la vérification

---

# Les lanceurs d’alertes dans la Loi pour une République numérique

**Les lanceurs d'alertes ou « white hats » interpellent de plus en plus les medias depuis quelques années. Ces hackers éthiques interviennent dans l'informatique et le numérique, ils veillent à avertir les responsables de la sécurité des SI des vulnérabilités de leurs systèmes d'information ou de leurs sites web.**

De plus, avec le développement de plates-formes de bug bounty comme YesWeHack, il était important de légaliser une pratique exposée à des sanctions pénales (ex : art. 323-1 du code pénal, 2 ans de prison et 60.000 euros d'amende). La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique vient préciser le cadre légal de leurs actions.

**L'AFFAIRE DE L'ANSES ET LE VOL DE DONNÉES**

Un journaliste-blogueur surnommé « Bluetouff » avait extrait, puis publié de nombreux fichiers confidentiels en pénétrant sur le site extranet de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES). Il a été condamné par la Cour d'appel de Paris le 5 février 2014, puis par la Cour de cassation le 20 mai 2015 pour maintien frauduleux dans le SI et vol de données. Le législateur, « alerté » de cette situation, a commencé par modifier l'article 323-3 du code pénal en y ajoutant les actions d'extraire, de détenir, de reproduire, de transmettre frauduleusement des données (Loi n°2015-912 du 24 juillet 2015).

**LA PREMIÈRE MOUTURE VISÉE À L'ARTICLE 20 SEPTIE DE LA LOI**

C'est un amendement du 15 janvier 2016, dit « Bluetouff » qui a relancé les débats sur le sujet ayant abouti à la proposition d'ajouter un nouvel alinéa à l'article 323-1 du code pénal, ainsi rédigé :
*« Toute personne qui a tenté de commettre ou commis le délit prévu au présent article est exempte de peine si elle a immédiatement averti l'autorité administrative ou judiciaire ou le responsable du système de traitement automatisé de données en cause d'un risque d'atteinte aux données ou au fonctionnement du système. »*

Il était censé protéger les lanceurs d'alerte lorsqu'ils veillent *« à avertir les responsables de traitement des failles dans leurs systèmes.* » Or, cette rédaction laissait dubitatifs les juristes et posait plus de questions qu'elle n'en résolvait, notamment : quelle autorité saisir et par quel canal (appel téléphonique à la police, courrier postal ou électronique à une cour d'appel ou à la CNIL, etc.) ? Que se passe-t-il après l'avertissement et surtout, si entre temps le responsable du SI a porté plainte, ou encore si le lanceur d'alertes diffuse les informations sur l'internet pour se faire de la publicité ? De plus, exemption de peine ne signifie pas non inscription au casier judiciaire de la condamnation. Pourtant, une décision du 9 septembre 2009 a jugé que tout accès non autorisé à un SI constitue un trouble manifestement illicite alors même que cela peut permettre d'éviter des atteintes ultérieures aux données ou au fonctionnement du système.

**LA PROTECTION NOUVELLE DES LANCEURS D'ALERTE**

L'article 47 de la nouvelle loi prévoit que le code de la défense soit complété par un article L. 2321-4 ainsi rédigé : « *Art. L. 2321-4.-Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'*article 40 du code de procédure pénale *n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données. »*
*« L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée. »*
*« L'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa du présent article aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information.* »

L'information vise les vulnérabilités de sécurité des SI (art. 323-1) mais sans doute pas les autres délits informatiques prévus aux articles 323-2 (entraver et fausser le fonctionnement d'un SI), 323-3 (introduction de données, extraction, transmission, reproduction, suppression, modification des données) et 323-3-1 (programmes malveillants), ainsi que les infractions commises en groupe ou en bande organisée. Ces dernières infractions peuvent, en effet, causer des dommages importants au responsable du SI. L'un des points essentiels sera de déterminer les conditions de la *bonne foi* de la personne ayant détecté la vulnérabilité, étant observé que si la personne agit dans le cadre d'un programme de Bug bounty, on peut supposer que la bonne foi est présumée dans la mesure où le programme est déterminé par l'utilisateur, c'est à dire l'entreprise (idem pour la société qui réalise un Pentest).Il en va de même, si l'informateur a pénétré dans le site et qu'il s'en retire dès le moment où il s'aperçoit qu'il accède à une partie du site ou des données protégées…[lire la suite]

---

Notre métier : Sensibiliser les décideurs et les utilisateurs. Vous apprendre à vous protéger des pirates informatiques, vous accompagner dans votre mise en conformité avec la CNIL et le règlement Européen sur la Protection des Données Personnelles (RGPD). (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

# Original de l'article mis en page : Les lanceurs d'alertes dans la Loi pour une République numérique