

Les sept étapes d'une cyberattaque réussie

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer



Denis JACOPINI
vous informe

Les sept étapes d'une cyberattaque réussie

Les cyberattaques avancées peuvent rester indétectées sur un réseau durant plus de 200 jours en moyenne. Cela laisse amplement le temps aux cybercriminels de collecter et voler des données privées, de surveiller les communications et de cartographier le réseau.

Comme toute entreprise ambitieuse, une cyberattaque réussie exige une planification soignée et une exécution précise. Ce que les piratages efficaces ont en commun est le fait de pouvoir attendre à couvert le bon moment pour frapper. Et si les attaques ont recours à diverses méthodes, elles ont généralement plusieurs étapes similaires en commun. Afin de pouvoir parer les cyberattaques, il est important de comprendre quelles sont ces étapes. Décryptons ensemble leur schéma type.

Voici les sept étapes d'une cyberattaque réussie :

1. Reconnaissance
2. Exploration
3. Accès et élévation
4. Exfiltration
5. Attente
6. Assaut
7. Obfuscation ...[lire la suite et les détails]

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *Les sept étapes d'une cyberattaque réussie – Global Security Mag Online*

Vous êtes victime de Cyberarnaques ? Redoublez de prudence car la justice pourrait bien vous donner tort !





Vous êtes victime de Cyberarnaques ? Redoublez de prudence car la justice pourrait bien vous donner tort !

**Paiement frauduleux en ligne : négligence de la victime de phishing...
Vous êtes victime de Cyberarnaques ? Redoublez de prudence car la justice pourrait bien vous donner tort !**

Par un arrêt du 25 octobre 2017, la Cour de cassation a annulé le jugement de la juridiction de proximité de Calais qui avait ordonné à la Caisse du crédit mutuel de Calais de rembourser les sommes prélevées sur le compte d'une victime d'une opération de phishing. La Cour reproche au tribunal de s'être ainsi déterminé sans rechercher si la victime en cause « *n'aurait pas pu avoir conscience que le courriel qu'elle avait reçu était frauduleux et si, en conséquence, le fait d'avoir communiqué son nom, son numéro de carte bancaire, la date d'expiration de celle-ci et le cryptogramme figurant au verso de la carte, ainsi que des informations relatives à son compte SFR permettant à un tiers de prendre connaissance du code 3D Secure ne caractérisait pas un manquement, par négligence grave, à ses obligations mentionnées à l'article L. 133-16 du code monétaire et financier* »....[lire la suite]

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

[Les 10 conseils pour ne pas se faire «hacker» pendant l'été](#)

[Les meilleurs conseils pour choisir vos mots de passe](#)

[Victime d'un piratage informatique, quelles sont les bonnes pratiques ?](#)

[Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?](#)

[Attaques informatiques : comment les repérer ?](#)

[block id="24760" title="Pied de page BAS"]

Source : Legalis | L'actualité du droit des nouvelles technologies | Paiement frauduleux en ligne : négligence de la victime de phishing

HTTPS ou le cadenas du navigateur ne veulent pas dire que le site est fiable !



HTTPS ou le
cadenas du
navigateur ne
veulent pas dire
que le site est
fiable !

Depuis plusieurs années j'entends des « professionnels » de l'informatique recommander à leur client de bien vérifier la présence d'un cadenas ou d'une adresse qui commence par « https ». Trop régulièrement échangent des données sensibles (tels que les passe mots de sites, numéros de CB...). Sais autre conseil, selon Denis JACOPINI, cette recommandation ne vaut rien.

Le Net Expert : Qu'est ce que le protocole HTTPS (HyperText Transfer Protocol Secure) ?

Denis JACOPINI : Le protocole HTTPS (HyperText Transfer Protocol Secure) est la combinaison du HTTP avec un protocole de chiffrement tel que le TLS ou le SSL. Il est particulièrement utilisé sur le Web pour les réseaux sociaux et dans les secteurs bancaires et de l'e-commerce pour sécuriser les pages sensibles (page d'authentification, mon compte, page de paiement).

Le Net Expert : Lorsqu'on navigue sur un site dont l'URL (l'adresse internet) commence par « https » (par exemple https://www.leonetexpert.fr), ceci ne veut pas dire que le site internet est de confiance ou fiable. Cela signifie simplement que la communication entre votre ordinateur et le site Internet sera chiffrée (cryptée) afin qu'un espion ou un pirate connecté sur votre WiFi ou votre LAN avec des outils d'espionnage numérique (un sniffier ou un Man In The Middle) ne puisse « écouter » ou « capturer » le contenu de l'échange.

Enfin, une boutique en ligne qui affiche des conditions générales de vente et qui indique que le site internet est soumis à la législation française (et non à celle de l'Union Européenne) qui devrait inclure la protection des données personnelles, mais qui n'a pas de cadenas sur son site, n'a pas de certificat SSL et utilise un serveur hébergeant gratuitement.

Tout comme dans le monde des boutiques physiques il existe des cybercommerts sérieux et fiables mais si vous devez acheter un produit sur Internet et que vous le trouvez sur une boutique moins cher que partout ailleurs, poser des questions. Privileiez les boutiques en ligne dans des pays étrangers ou à l'étranger. En cas de litige, il sera difficile de faire valoir vos droits car les lois françaises très protectrices des consommateurs. A moins de faire partie d'un tiers de confiance, évitez d'acheter sur les boutiques Internet situées dans des pays étrangers ou à l'étranger. En cas de litige, il sera difficile de faire valoir vos droits car les lois françaises très protectrices des consommateurs.

Certes avoir un cadenas sur votre navigateur et une adresse internet avec un https sont essentiels pour communiquer des informations confidentielles telles que vos mots de passe ou vos coordonnées de carte bancaire mais la réputation de la boutique ou sa situation géographique sont des éléments tout aussi importants.

Les informations contenues dans nos publications sont destinées à vous sensibiliser et augmenter votre niveau de prudence et en aucun cas dans un but de vous inciter à les utiliser dans un but malveillant.

LE NET EXPERT

- ACCOMPAGNEMENT RPO (ETAT DES LIEUX - MISE EN CONFORMITE)
- ANALYSE DE VOTRE ACTIVITÉ
- CARTOGRAPHIE DES RISQUES ET DES DOSSIERS
- IDENTIFICATION DES RISQUES
- ANALYSE DE RISQUES (PIA / DPA)
- MISE EN PLACE D'UN RPO (DOSSIER D'ÉVÉNEMENTS)
- SUIVEZ DE L'ÉVOLUTION DE VOS TRAITEMENTS
- FORMATION DES PERSONNELS :

 - CYBERCRIMINALITÉ
 - PROTECTION DES DONNÉES PERSONNELLES
 - À LA FONCTION DE DPO

- RECHERCHE DE PROOF OF CONCEPT (PoC) / PROOF OF VULNERABILITY (PoV)

- COORDINATES (Photos / E-mails / Fichiers)
- TÉLÉPHONES (Recuperation de Photos / SMS)
- ECRANS (Captures d'écran)
- EXPERTISES & TESTS (certifié ISO 27001)
- TECHNIQUES D'ANALYSES INVESTIGATIVES
- SECURITÉ INFORMATIQUE
- SYSTÈMES DE VOTES ELECTRONIQUES

Denis d'un Expert à contacter nous



Réagissez à cet article

Notre Expert, Denis JACOPINI, est assurément spécialisé en Cybercriminalité, Recherche de preuves et en Protection des données personnelles. Diplômé en Cybercriminalité (Université de Paris 8), en Droit de l'Informatique et des Technologies (Paris 8), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27001), Denis JACOPINI est aussi formateur inscrit auprès de la CERTIF (Numéro formateur #93 84 63041 54).

Source : Denis JACOPINI

Cybermenaces : Quelques signaux d'alerte à connaître



Cybermenaces : Quelques signaux d'alerte à connaître

Un email, une pièce jointe... une infection informatique. Le scénario est désormais classique : qu'il s'agisse d'une PME ou d'une entreprise de plus grande taille, l'erreur humaine est à la base de 75% des problèmes de sécurité.

En quelques années, la cybermenace est passée du statut de vague thème de fiction à un celui de vrai sujet de préoccupation pour l'entreprise – exemples concrets à l'appui. Il est indispensable que les collaborateurs soient formés à décrypter en amont les signaux d'alerte, d'autant qu'ils sont souvent les premiers vecteurs de propagation.

Un chiffre plutôt qu'un long discours : 80% (NDLR en approche des 90%) des infections arrivent par e-mail tandis que, le plus souvent, l'infection se déclenche par téléchargement d'une pièce jointe – le mode de diffusion de prédilection des rançongiciels.

Un e-mail malveillant a :

1. Un expéditeur mystère
2. Un objet très alarmiste
3. Une pièce jointe inattendue
4. Une demande inhabituelle
5. Un site inconnu, soi-disant sécurisé
6. Quand c'est trop beau pour être vrai

[lire la suite]

LE NET EXPERT

- ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX → MISE EN CONFORMITÉ)
 - ANALYSE DE VOTRE ACTIVITÉ
 - CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES
 - IDENTIFICATION DES RISQUES
 - ANALYSE DE RISQUE (PIA / DPIA)
 - MISE EN CONFORMITÉ RGPD de vos traitements
 - SUIVI de l'évolution de vos traitements
- FORMATIONS / SENSIBILISATION :
 - CYBERCRIMINALITÉ
 - PROTECTION DES DONNÉES PERSONNELLES
 - AU RGPD
 - À LA FONCTION DE DPO
- RECHERCHE DE PREUVES (outils Gendarmerie/Police)
 - ORDINATEURS (Photos / E-mails / Fichiers)
 - TÉLÉPHONES (récupération de Photos / SMS)
 - SYSTÈMES NUMÉRIQUES
- EXPERTISES & AUDITS (certifié ISO 27005)
 - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
 - SÉCURITÉ INFORMATIQUE
 - SYSTÈMES DE VOTES ÉLECTRONIQUES

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- **Mises en conformité RGPD** ;
- Accompagnement à la mise en place de DPO ;
- **Formations** (et sensibilisations) à la **cybercriminalité** (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- **Recherche de preuves** téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- **Expertises de systèmes de vote électronique** ;



[Contactez-nous](#)

Réagissez à cet article

Source : *Cybermenaces : 6 signaux d'alerte à connaître*

Envoyé spécial sur les Cyberattaques : les braqueurs de l'ombre – 14 décembre 2017 (France 2)



**Envoyé spécial
sur les
Cyberattaques
les
braqueurs
l'ombre – 14
décembre 2017
(France 2)**

Les hold-up 2.0 par des « rançongiciels », logiciels de rançon, se multiplient : en France, une entreprise sur deux aurait déjà été piratée de cette façon. Enquête du magazine « Envoyé spécial » sur un fléau invisible en pleine explosion.

Merci à Clément Le Goff et Guillaume Beaufils pour ce beau travail d'enquête. Tout est vrai, et encore, tout n'est pas dit. Quelles conséquences avec les objets connectés, bientôt principaux cadeaux de noël, les voitures connectées, et tous les outils informatiques ou algorithmiques dont leurs usages peuvent être détournés à des fins malveillantes.

Depuis plusieurs années, Denis JACOPINI essaie par le biais de conférences ou en participant à des émissions de radio ou de TV (D8, LCI, NRJ12, Sud Radio, Sputnik...) de sensibiliser la population à ces risques afin de les aider à anticiper et éviter le plus possible ces attaques en leur apprenant à se protéger des pirates informatiques.

Avec un tel reportage, j'espère que le plus grand nombre de personnes sera sensibilisé de manière à enrayer ce phénomène incoercible.

Seul petit bémol dans ce reportage. Beaucoup auront entendu et retenu les recommandations de la police qui sont qu'il ne faut pas payer la rançon lorsqu'un pirate prend vos données en otage. Je compléterais par le fait qu'il ne faut pas payer si vous avez la possibilité d'utiliser des sauvegardes ou si les conséquences sont minimales. Par contre, si la vie d'une entreprise est en jeu et la seule chance restante (même infime) pour sauver l'entreprise est de payer la rançon, ne pas la payer risquerait bien de vous être reproché... à moins que ça soit, comme dans le reportage un coup de grâce accepté par désespoir.

Corriger le message afin de ne pas induire les entreprises en erreur me paraît indispensable.

LE NET EXPERT

- ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX → MISE EN CONFORMITÉ)
 - ANALYSE DE VOTRE ACTIVITÉ
 - CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES
 - IDENTIFICATION DES RISQUES
 - ANALYSE DE RISQUE (PIA / DPIA)
 - MISE EN CONFORMITÉ RGPD de vos traitements
 - SUIVI de l'évolution de vos traitements
 - FORMATIONS / SENSIBILISATION :
 - CYBERCRIMINALITÉ
 - PROTECTION DES DONNÉES PERSONNELLES
 - AU RGPD
 - À LA FONCTION DE DPO
 - RECHERCHE DE PREUVES (outils Gendarmerie/Police)
 - ORDINATEURS (Photos / E-mails / Fichiers)
 - TÉLÉPHONES (récupération de Photos / SMS)
 - SYSTÈMES NUMÉRIQUES
 - EXPERTISES & AUDITS (certifié ISO 27005)
 - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
 - SÉCURITÉ INFORMATIQUE
 - SYSTÈMES DE VOTES ÉLECTRONIQUES

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en Cybercriminalité, Recherche de preuves et en Protection des données personnelles. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- **Mises en conformité RGPD** ;
- Accompagnement à la mise en place de DPO ;
- **Formations** (et sensibilisations) à la **Cybercriminalité** (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- **Recherche de preuves** téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- **Expertises de systèmes de vote électronique** ;

Les hold-up 2.0 par des « rançongiciels », logiciels de rançon, se multiplient : en France, une entreprise sur deux aurait déjà été piratée de cette façon. Enquête du magazine « Envoyé spécial » sur un fléau invisible en pleine explosion.

Depuis plusieurs années, Denis JACOPINI essaie par le biais de conférences ou en participant à des émissions de radio ou de TV (D8, LCI, NRJ12, Sud Radio, Sputnik) de sensibiliser la population à ces risques afin de les aider à anticiper et éviter ces attaques.

Merci à Clément Le Goff et Guillaume Beaufils

Avec un tel reportage, j'espère que

LE NET EXPERT

- ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX → MISE EN CONFORMITÉ)
 - ANALYSE DE VOTRE ACTIVITÉ
 - CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES
 - IDENTIFICATION DES RISQUES
 - ANALYSE DE RISQUE (PIA / DPIA)
 - MISE EN CONFORMITÉ RGPD de vos traitements
 - SUIVI de l'évolution de vos traitements
 - FORMATIONS / SENSIBILISATION :
 - CYBERCRIMINALITÉ
 - PROTECTION DES DONNÉES PERSONNELLES
 - AU RGPD
 - À LA FONCTION DE DPO
- RECHERCHE DE PREUVES (outils Gendarmerie/Police)
 - ORDINATEURS (Photos / E-mails / Fichiers)
 - TÉLÉPHONES (réécriture de Photos / SMS)
 - SYSTÈMES NUMÉRIQUES
- EXPERTISES & AUDITS (certifié ISO 27005)
 - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
 - SÉCURITÉ INFORMATIQUE
 - SYSTÈMES DE VOTES ÉLECTRONIQUES

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

Prédictions cybersécurité 2018



Prédictions
cybersécurité
2018

En 2018, les cybercriminels vont continuer à exploiter les faiblesses inhérentes à la nature humaine pour dérober des informations personnelles, avec des changements significatifs dans les techniques de cyberattaques. Découvrez les grandes lignes de ces tendances qui rythmeront l'année 2018 selon Proofpoint.

☒ L'email restera le vecteur de cyberattaque le plus utilisé

☒ Vol de cryptomonnaie : de nouvelles menaces aussi répandues que les chevaux de Troie

☒ Le facteur humain, toujours au cœur des cyberattaques

☒ La menace grandissante des bots sur les réseaux sociaux

[cliquez pour plus de détails]

LE NET EXPERT

- ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX → MISE EN CONFORMITÉ)
 - ANALYSE DE VOTRE ACTIVITÉ
 - CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES
 - IDENTIFICATION DES RISQUES
 - ANALYSE DE RISQUE (PIA / DPIA)
 - MISE EN CONFORMITÉ RGPD de vos traitements
 - SUIVI de l'évolution de vos traitements
 - FORMATIONS / SENSIBILISATION :
 - CYBERCRIMINALITÉ
 - PROTECTION DES DONNÉES PERSONNELLES
 - AU RGPD
 - À LA FONCTION DE DPO
- RECHERCHE DE PREUVES (outils Gendarmerie/Police)
 - ORDINATEURS (Photos / E-mails / Fichiers)
 - TÉLÉPHONES (récupération de Photos / SMS)
 - SYSTÈMES NUMÉRIQUES
- EXPERTISES & AUDITS (certifié ISO 27005)
 - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
 - SÉCURITÉ INFORMATIQUE
 - SYSTÈMES DE VOTES ÉLECTRONIQUES

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

Source : *Prédictions cybersécurité 2018 – Global Security Mag Online*

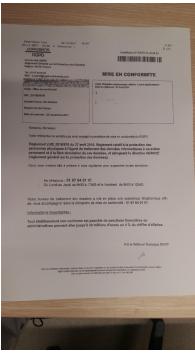
Alerte à la fausse « Mise en conformité RGPD »

 **Alerte à la fausse « Mise en conformité RGPD »**

Des entreprises ont reçu par fax et par téléphone, en particulier ces derniers jours, des messages pour une « mise en conformité » avec le règlement européen sur la protection des données personnelles (dit « RGPD »). Le message, alarmiste et pouvant faire penser à une mise en demeure administrative, insiste sur les sanctions financières encourues.

Ces messages peuvent avoir pour but de vous faire appeler un numéro de téléphone surtaxé, de vous faire signer un engagement frauduleux pour une « mise en conformité Informatique et Libertés (ou RGPD) » ou de collecter des informations sur votre organisation pour préparer une escroquerie ou une attaque informatique.

La CNIL n'est, bien entendu, pas à l'origine de ces messages.
N'y répondez pas ! En cas de doute, vous pouvez contacter la vraie CNIL au 01 53 73 22 22.



Exemple de courrier RGPD frauduleux

- * En cas de doute, contactez la CNIL au 01 53 73 22 22 ;
- * Signalez cette arnaque au 0 811 02 17 ou sur le site www.internet-signalement.fr ;
- * Consulter le site de l'agence nationale de sécurité des systèmes d'information (ANSSI) www.anssi.gouv.fr ;
- * Consulter le site du centre gouvernemental d'alerte et de lutte contre les attaques informatiques CERT-FR www.cert-ssi.gouv.fr ;
- * Déposez plainte si vous le souhaitez auprès des services de police ou de gendarmerie ou faites une déclaration directement sur le site de pré-plainte en ligne https://www.pre-plainte-en-ligne.gouv.fr ;
- * Restez vigilant.

LE NET EXPERT

- * MISE EN CONFORMITÉ RGPD / CNIL
- * DROIT RÔTIE ET CARTOGRAPHIE DE VOS TRAITEMENTS
- * MISE EN CONFORMITÉ RGPD / VOS TRAITEMENTS
- * SUIVI de l'évolution de vos traitements
- * FORMATIONS / SENSIBILISATION :

 - Protection des données personnelles
 - Protection des données sensibles
 - Protection des données biométriques
 - Protection des données financières
 - Protection des données de santé
 - Protection des données géolocalisées
 - Protection des données commerciales
 - Protection des données industrielles
 - Protection des données culturelles
 - Protection des données éducatives
 - Protection des données administratives
 - Sécurité informatique
 - Systèmes de votes électroniques

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en Cyberrriminalité, Recherche de preuves et en Protection des données personnelles. Diplômé en Cybercriminalité (Droit, Sécurité de l'Information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005). Denis JACOPINI est aussi formateur inscrit auprès de la DNITFP (Numéro formateur n°93 84 03841 84).



Le Net Expert
INFORMATIQUE
Contactez-nous

Rédigé à cet article

Source : Vigilance – « *Mise en conformité RGPD* » | CNIL

Alerte : Facebook Messenger pourrait propager un virus



Alerte : Facebook Messenger pourrait propager un virus

Les applications de messageries instantanées sont souvent la cible de virus informatiques. Facebook Messenger n'a pas échappé à cette règle: selon Le Monde Informatique, un logiciel malveillant (« malware », ndlr) se propage actuellement sur le réseau social.

C'est le chercheur David Jacoby, de la société informatique spécialisée dans la sécurité des systèmes d'information, qui a pu détecter ce virus. Le principe est classique: un de vos contacts envoie une vidéo nommée « David Video ». David Jacoby précise au *Monde Informatique*: « Lorsque la victime clique sur la fausse vidéo, le malware redirige vers un éventail de sites énumérant leur navigateur, système d'exploitation et d'autres informations vitales. Selon leur OS, ils sont redirigés vers d'autres sites web ».

Ce virus, qui ne menace pas l'appareil en lui-même, peut installer des logiciels malveillants à l'insu de l'utilisateur. En outre, il peut également récupérer les données personnelles...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficience maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-nous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles> (Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle)



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Source : *Un virus informatique détecté sur Facebook Messenger*

Attention aux fausses société d'assistance informatique !



Attention
aux fausses
sociétés
d'assistance
informatique

Les cybercriminels présentent la particularité d'être inventifs et très opportunistes. La médiatisation de la cyberattaque WannaCry a créé une peur que des hackers mal intentionnés ont parfaitement su utiliser.

Ainsi, les spams (courriels indésirables, généralement publicitaires) ont augmenté de 57% au deuxième trimestre 2017 d'après Kaspersky Lab. Avec une particularité : de nombreux courriels contenaient « *des offres de services de lutte contre WannaCry, des conseils pour éviter d'infection ainsi que des invitations à des séminaires de formation* ». Les escrocs en ont profité pour envoyer de fausses notifications, au nom d'éditeurs connus de logiciels, qui signalaient au destinataire que son ordinateur avait été infecté et qu'il fallait cliquer sur un lien pour installer une mise à jour. Problème : ce lien menait sur une page de *phishing*, c'est-à-dire un formulaire incitant les victimes à entrer des informations personnelles, utilisées ensuite pour effectuer une usurpation d'identité...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficience maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-nous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles> (Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle)



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité », « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Source : *Cyberattaques, spams, malwares : les cybercriminels n'ont pas chômé au deuxième trimestre*

Un nouveau ransomware, Defray, cible l'éducation et la santé



Les chercheurs Proofpoint ont récemment analysé un nouveau ransomware, nommé Defray. Durant le mois d'août, ils ont observé plusieurs attaques ciblées, visant notamment les secteurs de la santé, de l'éducation, de l'industrie et de l'informatique.

« Defray » a été choisi en rapport avec le nom d'hôte du serveur de commande et de contrôle (C&C) de la première attaque observée :

defrayable-listings[.]000webhostapp[.]com Par coïncidence, le terme « defray » signifie fournir de l'argent pour payer une partie d'un coût, bien que ce dont les victimes doivent s'acquitter ne soit pas tout à fait clair.

La distribution de Defray présente plusieurs caractéristiques :

- Defray est diffusé via des documents Word dans des pièces jointes d'emails
 - Les pièges sont conçus sur mesure pour attirer toutes les victimes potentielles
 - Les destinataires sont des individus ou bien des groupes d'individus, par exemple, group@ ou websupport@
 - Les pays les plus touchés sont le Royaume-Uni et les États-Unis
- [Global Security Mag Online]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficience maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles> (Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle)



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité », « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Source : *Defray, le nouveau ransomware qui cible l'éducation et la santé – Global Security Mag Online*